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 lance en 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 en las instalaciones. Puede habilitar el acceso a dispositivos remotos desde la VPC mediante la creación de una conexión de AWS Site-to-Site VPN (Site-to-Site VPN) y la configuración del enrutamiento para que el tráfico pase a través de la conexión.

Aunque el término conexión de VPN es un término general, en esta documentación, hace referencia a la conexión entre su VPC y su propia red local. VPN de sitio a sitio admite conexiones de VPN con cifrado Internet Protocol Security (IPsec).

Contenido

Conceptos

A continuación, se incluyen los conceptos clave de Site-to-Site VPN:

- Conexión de VPN: conexión segura entre el equipo que se encuentra en las instalaciones y sus VPC.
- 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.
- Gateway de cliente: recurso de AWS que proporciona información a AWS sobre su dispositivo de gateway de cliente.
- Dispositivo de gateway de cliente: dispositivo físico o aplicación de software que se encuentra en su extremo de la conexión de Site-to-Site VPN.

- Puerta de enlace de destino: término genérico para el punto de conexión VPN en el lado de Amazon de la conexión Site-to-Site VPN.
- Puerta de enlace privada virtual: es el punto de conexión VPN en el lado de Amazon de la conexión Site-to-Site VPN que se puede adjuntar a una única VPC.
- Puerta de enlace de tránsito: un hub de tránsito que se puede utilizar para interconectar varias VPC y redes en las instalaciones y como punto de conexión VPN para el lado de Amazon de la conexión Site-to-Site VPN.

Características de Site-to-Site VPN

Se admiten las siguientes características en las conexiones de VPN AWS Site-to-Site VPN:

- 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 gateway de cliente para su conexión de AWS Site-to-Site VPN.
- ASN de 2 bytes para puerta de enlace de cliente (CGW) comprendidos entre 1 y 65535. Para obtener más información, consulte Opciones de gateway de cliente para su conexión de AWS Site-to-Site VPN.
- Métricas de CloudWatch
- 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
- Compatibilidad de IPv6 con AWS Site-to-Site VPN
  - IPv6 para direcciones IP de túnel interno (IP de paquete)
  - IPv6 para direcciones IP de túnel externo (IP de túnel) en Transit Gateway y WAN en la nube
- Compatibilidad total con la migración de IPv6 con las siguientes combinaciones:
  - IP de túnel externo de IPv6 con IP de paquete interno de IPv6 (IPv6 en IPv6)
  - IP de túnel externo de IPv6 con IP de paquete interno de IPv4 (IPv4 en IPv6)

Limitaciones de Site-to-Site VPN

Las conexiones de Site-to-Site VPN tienen las siguientes limitaciones.

- El tráfico IPv6 no es compatible con las conexiones VPN en una gateway privada virtual. IPv6 para IP de túnel externo solo se admite en Transit Gateway y WAN en la nube.
- Una conexión de Site-to-Site VPN no es compatible con la detección de la MTU de la ruta.
- Una conexión de Site-to-Site VPN no admite tráfico de IPv4 y de IPv6 simultáneamente. Necesita conexiones de Site-to-Site VPN independientes para transportar los paquetes IPv4 e IPv6.
- Las conexiones privadas de VPN IP no admiten direcciones IPv6 para las IP de túnel externo.
- No puede modificar una conexión de VPN IPv4 existente para usar IPv6. Debe eliminar la conexión existente y crear una nueva.

Además, debe tener en cuenta lo siguiente cuando utilice Site-to-Site VPN:

- Al conectar las VPC a una red en las instalaciones común, se recomienda utilizar bloques de CIDR no superpuestos para las redes.

Recursos de Site-to-Site VPN

Puede crear los recursos de Site-to-Site VPN, acceder a ellos y administrarlos desde cualquiera de las siguientes interfaces:

- Consola de administración de AWS— proporciona una interfaz web que se puede utilizar para acceder a los recursos de Site-to-Site VPN.
- AWS Command Line Interface (AWS CLI): proporciona comandos para numerosos servicios de AWS, como Amazon VPC, y es compatible con Windows, macOS y Linux. Las líneas de comandos de AWS Site-to-Site VPN se incluyen en la referencia general de líneas de comandos de EC2.
  - Para obtener información general acerca de estas interfaces de líneas de comandos, consulte AWS Command Line Interface.
  - Para ver la lista de comandos de EC2 disponibles, incluidos los comandos de Site-to-Site VPN, consulte Referencia de la línea de comandos de EC2.

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

- SDK de AWS: proporcionan API específicas de cada lenguaje y se encargan de muchos de los detalles de la conexión, como el cálculo de firmas, el control de reintentos de solicitud y el control de errores. Para obtener más información, consulte SDK de AWS.
- 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, consulte la referencia de las API de Amazon EC2.

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 de AWS Site-to-Site VPN y Accelerated Site-to-Site VPN Connection.

Se le cobra la transferencia de datos desde Amazon EC2 a Internet. Para obtener más información, consulte la sección Transferencia de datos en la página Precios bajo demanda de Amazon EC2.

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 más información, consulte Precios de AWS Global Accelerator.

No hay cargos adicionales por el uso de direcciones IPv6 con las conexiones de VAPN de Site-to-Site VPN.

Cómo funciona AWS Site-to-Site VPN

Las conexiones de Site-to-Site VPN constan de lo siguiente:

- 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

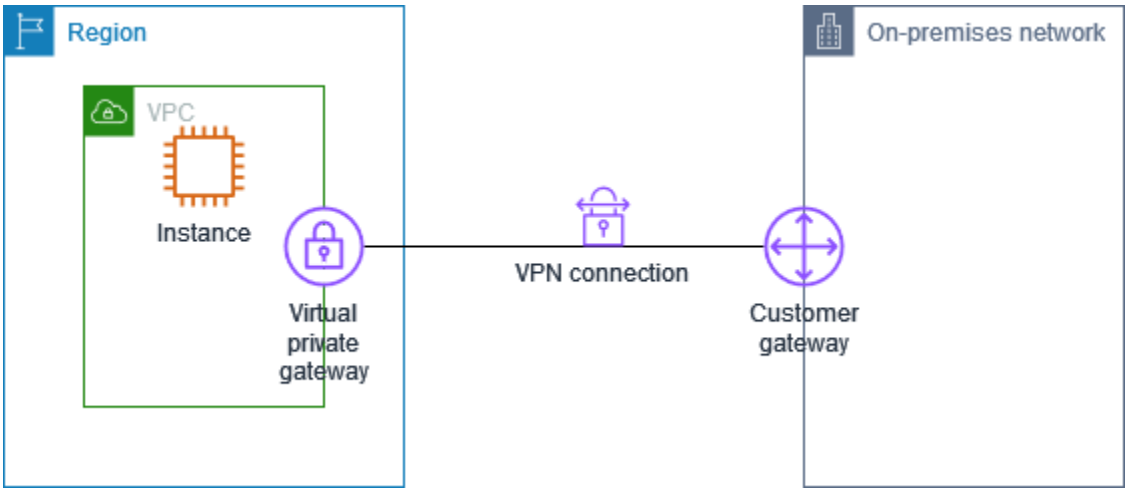
Una conexión de VPN ofrece dos túneles de VPN entre una puerta de enlace privada virtual o una puerta de enlace de tránsito en el lado de AWS y una puerta de enlace de cliente en las instalaciones.

Para obtener más información sobre las cuotas de Site-to-Site VPN, consulte AWS Site-to-Site VPNCuotas de .

Gateway privada virtual

La gateway privada virtual es el concentrador VPN que se encuentra en el extremo de Amazon de la conexión de Site-to-Site VPN. Debe crear una puerta de enlace privada virtual y conectarla a una nube privada virtual (VPC) con recursos que deben acceder a la conexión de Site-to-Site 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

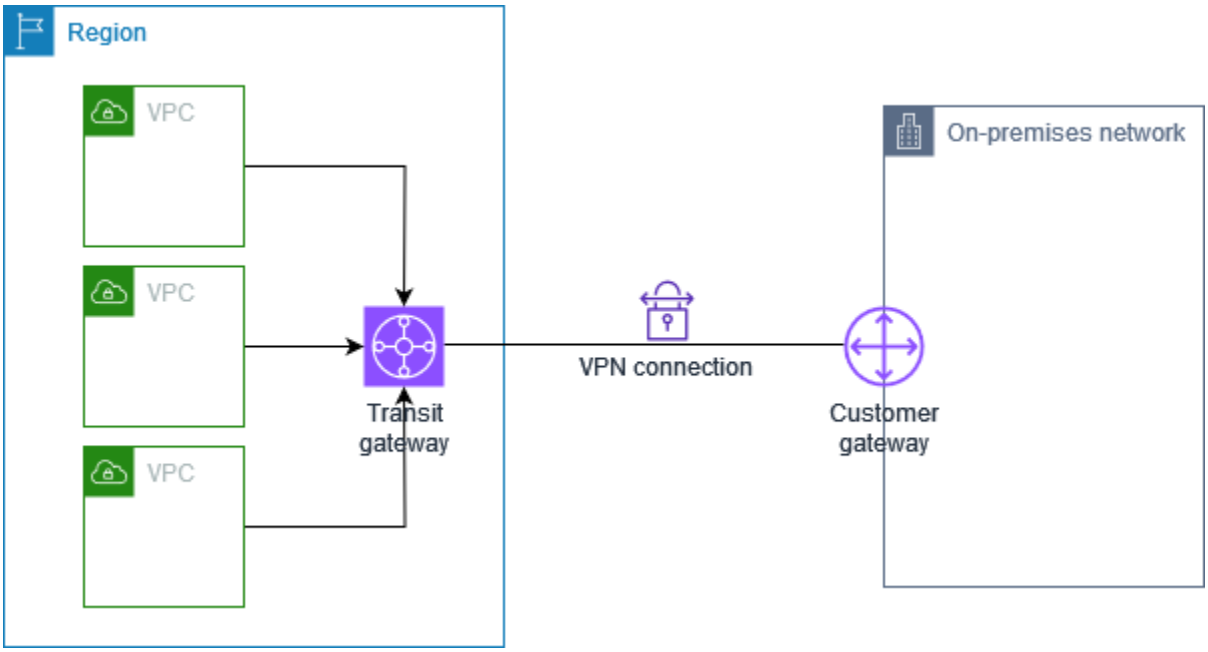
crea con el ASN predeterminado (64 512). No se puede cambiar el ASN una vez que ha creado la gateway privada virtual. Para comprobar el ASN de su puerta de enlace privada virtual, consulte sus detalles en la página Puertas de enlace privadas virtuales de la consola de Amazon VPC o utilice el comando de AWS CLI describe-vpn-gateways.

> **Note**
>
> Las puertas de enlace privadas virtuales no admiten IPv6 para conexiones de Site-to-Site VPN. Si necesita compatibilidad con IPv6, use una puerta de enlace de tránsito o la WAN en la nube para la conexión de VPN.

Puerta de enlace de tránsito

Un puerta de enlace de tránsito es un hub de tránsito que puede utilizar para interconectar sus VPC y redes en las instalaciones. Para obtener más información, consulte Gateways de tránsito de Amazon VPC. Puede crear una conexión de Site-to-Site VPN como una asociación de la gateway de tránsito.

El siguiente diagrama muestra una conexión de VPN entre varias VPC y su red en las instalaciones utilizando una puerta de enlace de tránsito. La puerta de enlace de tránsito tiene tres conexiones de VPC y una conexión de VPN.



La conexión de Site-to-Site VPN en una puerta de enlace de tránsito puede admitir el tráfico de IPv4 o IPv6 en los túneles de VPN (direcciones IP internas). Además, las puertas de enlace de tránsito

admiten direcciones IPv6 para las direcciones IP de túnel externas. Para obtener más información, consulte Tráfico de IPv4 e IPv6 en AWS Site-to-Site VPN.

Puede modificar la gateway de destino de una conexión de Site-to-Site VPN entre una gateway privada virtual y una gateway 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

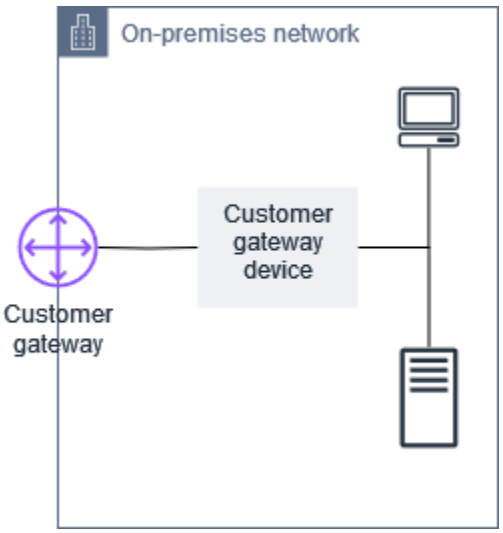
Un dispositivo de gateway de cliente es un dispositivo físico o una aplicación de software que se encuentra en su extremo de la conexión de Site-to-Site VPN. Puede configurar el dispositivo para que funcione con la conexión de Site-to-Site VPN. Para obtener más información, consulte dispositivos de puerta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

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

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

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 gateway del cliente, proporciona información sobre el dispositivo a AWS. Para obtener más información, consulte the section called "Opciones de gateway de cliente".



Para utilizar Amazon VPC con una conexión de Site-to-Site VPN, usted o su administrador de red también deberán configurar la aplicación o el dispositivo de gateway de cliente en la red remota. Cuando crea la conexión de Site-to-Site VPN, la información de configuración necesaria se la proporcionamos nosotros, mientras que es el administrador de red el que normalmente lleva a cabo esta configuración. Para obtener información sobre los requisitos y la configuración de la gateway de cliente, consulte dispositivos de puerta de enlace de cliente de AWS Site-to-Site VPN.

Puerta de enlace de cliente IPv6

Al crear una puerta de enlace de cliente para usarla con IP de túnel externo de IPv6, debe especificar una dirección IPv6 en lugar de una dirección IPv4. Puede crear una puerta de enlace de cliente IPv6 mediante la Consola de administración de AWS o la AWS CLI.

Para crear una puerta de enlace de cliente IPv6 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 dirección IPv6 debe ser una dirección IPv6 válida enrutable por Internet para el dispositivo de puerta de enlace de cliente.

Conexiones de VPN IPv6

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

- Túnel externo de IPv4 con paquetes internos de IPv4: la capacidad básica de VPN IPv4 que admite puerta de enlace privada virtual (VGW), puerta de enlace de tránsito (TGW) y WAN en la nube.
- Túnel externo de IPv4 con paquetes internos de IPv6: permite transporte y aplicaciones de IPv6 en el túnel de VPN. Compatible con TGW y WAN en la nube (no compatible con VGW).
- Túnel externo de IPv6 con paquetes internos de IPv6: permite la migración completa de IPv6 con direcciones IPv6 tanto para las IP de túnel externo como para las IP de los paquetes internos. Compatible con TGW y WAN en la nube.
- Túnel externo IPv6 con paquetes internos de IPv4: permite el direccionamiento del túnel externo de IPv6 y, al mismo tiempo, admite aplicaciones IPv4 antiguas en el túnel. Compatible con TGW y WAN en la nube.

Para crear una conexión de VPN con IP de túnel externo de IPv6, debe especificar `OutsideIPAddressType=Ipv6` al crear la conexión de VPN. AWS configura automáticamente las direcciones IPv6 de túnel externo para el extremo de AWS de los túneles de VPN.

Ejemplo de comando de la CLI para crear una conexión de VPN con IP de túnel externo de IPv6 e IP de túnel interno de IPv6:

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

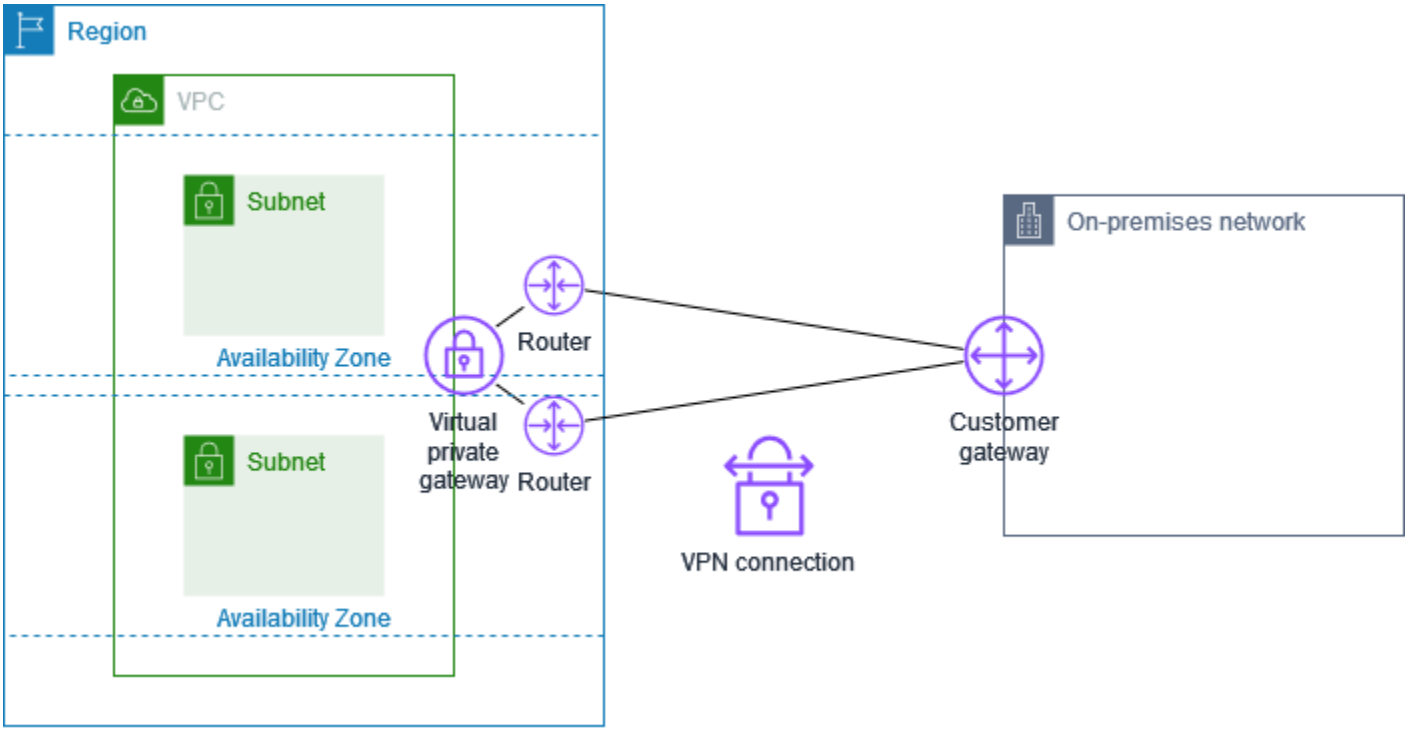
Puede ver las direcciones IPv6 asignadas a su conexión de VPN mediante el comando `describe-vpn-connection` de la CLI.

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

Utilice una conexión de Site-to-Site VPN para conectar la red remota a una VPC. Cada conexión Site-to-Site VPN tiene dos túneles y cada uno utiliza una dirección IP pública única. Es importante configurar ambos túneles para la redundancia. Cuando un túnel deja de estar disponible (por ejemplo, por tareas de mantenimiento), el tráfico de red se direcciona automáticamente al túnel disponible de esa conexión de 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 que sale desde la red

de las instalaciones a AWS utiliza ambos túneles. El tráfico que sale desde AWS a la red en las instalaciones prefiere uno de los túneles, pero puede conmutarse por error automáticamente al otro túnel si se produce un error en el lado de AWS.



Cuando cree una conexión de Site-to-Site VPN, tendrá que descargar un archivo de configuración específico para su dispositivo de gateway de cliente, que contendrá información para configurar el dispositivo y también cada túnel. Si lo desea, puede especificar usted mismo algunas de las opciones del túnel al crear la conexión de Site-to-Site VPN. De lo contrario, AWS proporciona los valores predeterminados.

> **Note**
>
> Los puntos de enlace de túnel de Site-to-Site VPN evalúan las propuestas de la gateway del cliente comenzando por el valor configurado más bajo de la siguiente lista, independientemente del orden de la propuesta de la gateway del cliente. Puede utilizar el comando `modify-vpn-connection-options` para restringir la lista de opciones que aceptarán los puntos de enlace de AWS. Para obtener más información, consulte lasopciones de modify-vpn-connection en la Referencia de la línea de comandos de Amazon EC2.

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 de conexión de la VPN considerará que el par está muerto 30 segundos después del primer keep-alive erróneo. 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 VPNOpciones de inicio de túnel de .

Valor predeterminado: `Clear`

Opciones de registro de VPN

Con los registros de Site-to-Site VPN, puede obtener acceso a detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones de 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 VPNRegistros de .

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 interior de CIDR IPv4

Intervalo de direcciones IPv4 internas (internas) para el túnel VPN. Pude especificar un bloque de CIDR de tamaño /30 desde el rango `169.254.0.0/16`. El bloque de CIDR debe ser único en todas las conexiones de Site-to-Site VPN que utilicen la misma gateway 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. Tenga cuidado cuando vuelva a utilizar el mismo bloque de CIDR en varias conexiones de Site-to-Site VPN de 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 de CIDR IPv4 de tamaño /30 del intervalo `169.254.0.0/16`.

Almacenamiento de claves compartidas previamente

Tipo de almacenamiento de la clave compartida previamente:

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

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

Túnel interior de CIDR IPv6

(Sólo conexiones VPN IPv6) Intervalo de direcciones IPv6 internas (internas) para el túnel VPN. Puede especificar un bloque CIDR de tamaño /126 desde el rango local `fd00::/8`. El bloque de CIDR debe ser único en todas las conexiones de Site-to-Site VPN que utilicen la misma gateway de tránsito. Si no especifica una subred IPv6, Amazon selecciona automáticamente una subred /128 de este intervalo. Independientemente de si especifica la subred o de si Amazon la selecciona, Amazon usa la primera dirección IPv6 utilizable de la subred para su extremo de la conexión y esta usa la segunda dirección IPv6 utilizable.

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

Tipo de dirección IP de túnel externo

Tipo de dirección IP de las direcciones IP de túnel externo. Puede especificar uno de los siguientes valores:

- `PrivateIpv4`: utilice una dirección IPv4 privada para implementar conexiones de Site-to-Site VPN a través de Direct Connect.
- `PublicIpv4`: (predeterminado) utilice direcciones IPv4 para las IP de túnel externo.
- `Ipv6`: utilice direcciones IPv6 para las IP de túnel externo. Esta opción solo está disponible para conexiones de VPN en una puerta de enlace de tránsito o de WAN en la nube.

Cuando lo selecciona `Ipv6`, AWS configura automáticamente las direcciones IPv6 de túnel externo para el extremo de AWS de los túneles de VPN. El dispositivo de puerta de enlace de cliente debe admitir el direccionamiento IPv6 y poder establecer túneles de IPsec con puntos de conexión IPv6.

Valor predeterminado: `PublicIpv4`

CIDR de red IPv4 local

(Solo conexión de VPN IPv4) Intervalo de CIDR utilizado durante la negociación de la fase 2 de IKE para el extremo del cliente (en las instalaciones) del túnel de VPN. Este intervalo se utiliza para proponer rutas, pero no impone restricciones de tráfico, ya que AWS utiliza exclusivamente VPN basadas en rutas. No se admiten VPN basadas en políticas, ya que limitarían la capacidad de AWS de admitir protocolos de enrutamiento dinámico y arquitecturas multirregionales. Debería

incluir los intervalos de IP de la red en las instalaciones que deben comunicarse a través del túnel de VPN. Se deben utilizar configuraciones de tablas de enrutamiento, NACL y grupos de seguridad adecuados para controlar el flujo de tráfico real.

Valor predeterminado: 0.0.0.0/0

CIDR de red IPv4 remota

(Solo conexión de VPN IPv4) Intervalo de CIDR utilizado durante la negociación de la fase 2 de IKE para el extremo de AWS de túnel de VPN. Este intervalo se utiliza para proponer rutas, pero no impone restricciones de tráfico, ya que AWS utiliza exclusivamente VPN basadas en rutas. AWS no admite VPN basadas en políticas porque carecen de la flexibilidad necesaria para escenarios de enrutamiento complejos y son incompatibles con características como las puertas de enlace de tránsito y rutas múltiples de igual costo (ECMP) de VPN. En el caso de las VPC, suele ser el intervalo de CIDR de la VPC. En el caso de las puertas de enlace de tránsito, podría incluir varios intervalos de CIDR procedentes de VPC conectadas o de otra red.

Valor predeterminado: 0.0.0.0/0

CIDR de red IPv6 local

(Sólo conexión VPN IPv6) Intervalo CIDR IPv6 en el lado de la gateway del cliente (local) que puede comunicarse a través de los túneles VPN.

Predeterminado:: :/0

CIDR de red IPv6 remota

(Solo conexión de VPN IPv6) El rango CIDR IPv6 en el lado de AWS que puede comunicarse a través de los túneles de 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, AES256, AES128-GCM-16, AES256-GCM-16

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.

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

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.

Valores predeterminados: SHA1, SHA2-256, SHA2-384, SHA2-512

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.

Valores predeterminados: SHA1, SHA2-256, SHA2-384, SHA2-512

Vida útil de la fase 1

> **Note**
>
> AWS inicia los cambios de clave con los valores de tiempo establecidos en los campos de vida útil de la fase 1 y 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 inicia los cambios de clave con los valores de tiempo establecidos en los campos de vida útil de la fase 1 y 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 tiempo de margen en segundos antes de que venza la duración de la fase 1 y 2, durante el cual el lado de AWS 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 de IKE para mostrar 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 VPNOpciones de inicio de túnel de .

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 Control del ciclo de vida del punto de conexión del túnel de AWS Site-to-Site VPN.

Valor predeterminado: `Off`

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

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

AWS Site-to-Site VPNOpciones de autenticación de túneles de

Puede utilizar claves compartidas previamente o certificados para autenticar los puntos de enlace del túnel de Site-to-Site VPN.

Claves previamente compartidas

Una clave compartida previamente (PSK) es la opción de autenticación predeterminada para túneles de Site-to-Site VPN. Al crear un túnel, puede especificar su propia PSK o permitir que AWS genere una automáticamente. Para almacenar la PSK, utilice uno de los siguientes métodos:

- Directamente en el servicio Site-to-Site VPN. Para obtener más información, consulte Dispositivos de una puerta de enlace de cliente de Site-to-Site VPN.
- En AWS Secrets Manager para mayor seguridad. Para obtener más información acerca de cómo utilizar Secrets Manager para almacenar una PSK, consulte Características de seguridad mejoradas con Secrets Manager.

A continuación, la PSK se utiliza para configurar el dispositivo de puerta de enlace de cliente.

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 poder generar y utilizar el certificado en el lado de AWS del punto de conexión del túnel de Site-to-Site VPN. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

> **Note**
>
> Para facilitar las rotaciones 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 API `CreateCustomerGateway` 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 VPN realiza una verificación de la cadena de certificados en el certificado de puerta de enlace de cliente al crear una VPN de certificado. Además de la entidad de certificación básica y las comprobaciones de validez, 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 VPNOpciones de inicio de túnel de

De forma predeterminada, el dispositivo de gateway de cliente debe mostrar los túneles de la conexión de Site-to-Site VPN generando tráfico e iniciando el proceso de negociación de Intercambio de claves de Internet (IKE). Puede configurar los túneles de VPN para especificar que AWS debe iniciar o reiniciar el proceso de negociación de IKE en su lugar.

Opciones de iniciación de IKE de túnel de VPN

Las siguientes opciones de iniciación de IKE están disponibles. Puede implementar una o ambas opciones en uno o ambos túneles de la conexión de 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 especificar que AWS deba iniciar el proceso de negociación de IKE en su lugar.
- 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 deba

reiniciar la sesión de IKE cuando se cumpla el tiempo de espera de DPD, o puede especificar que AWS no deba llevar a cabo ninguna acción cuando se cumpla el tiempo de espera de DPD.

Reglas y limitaciones

Se aplican las siguientes reglas y limitaciones:

- Para iniciar la negociación de IKE, AWS requiere la dirección IP pública del dispositivo de puerta de enlace de cliente. Si configuró la autenticación basada en certificados para su conexión de VPN y no especificó una dirección IP cuando creó el recurso de puerta de enlace de cliente en 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 Cambio de la puerta de enlace de cliente para una conexión de AWS Site-to-Site VPN.
- El inicio de IKE (acción de inicio) desde el extremo de AWS de la conexión de VPN solo se admite para IKEv2.
- Si utiliza el inicio de IKE desde el lado de AWS de la conexión de VPN, no incluye una configuración de tiempo de espera. Intentará establecer una conexión continuamente hasta que se establezca una. Además, el lado de AWS de la conexión de VPN reiniciará la negociación de IKE cuando reciba un mensaje de eliminación de SA desde la puerta de enlace de cliente.
- Si el dispositivo de gateway del cliente está detrás de un firewall u otro dispositivo que utilice la traducción de direcciones de red (NAT), debe tener una identidad (IDr) configurada. Para obtener más información acerca de IDr, consulte RFC 7296.

Si no configura la iniciación de IKE desde el extremo de AWS para el túnel de VPN y la conexión de VPN experimenta un periodo de inactividad (normalmente, 10 segundos, según su configuración), el túnel podría desactivarse. 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 opciones de túnel de AWS Site-to-Site VPN

reemplazos de los puntos de conexión de un túnel de AWS Site-to-Site VPN

Por motivos de redundancia, las conexiones de Site-to-Site VPN tienen dos túneles de VPN. A veces, uno o ambos puntos de conexión del túnel de VPN se sustituyen cuando AWS realiza actualizaciones del túnel o cuando usted modifica la conexión de 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

Modificación	Acción de la API	Impacto en el túnel
		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 actualización.

Sustituciones de puntos de conexión administrados por AWS

AWS Site-to-Site VPN es un servicio administrado que aplica actualizaciones periódicas a los puntos de enlace del túnel de 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 punto de conexión de túnel a un túnel de la 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.

Control del ciclo de vida del punto de conexión del túnel de AWS Site-to-Site VPN

El control del ciclo de vida del punto de conexión del túnel permite controlar el programa de sustituciones de los puntos de conexión y puede ayudar a minimizar las interrupciones de conectividad durante las sustituciones del punto de conexión del túnel administradas por AWS. Con esta característica, tiene la opción de elegir aceptar las actualizaciones administradas por AWS de los puntos de conexión del túnel en el momento que mejor le convenga 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 circunstancias, AWS podría aplicar actualizaciones críticas a los puntos de conexión del túnel de forma inmediata, aunque la característica de control del ciclo de vida del punto de conexión del túnel esté habilitada.

Temas

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 notificaciones de AWS Health sobre las próximas sustituciones de los puntos de conexión del túnel.
- El estado del mantenimiento pendiente, junto con las marcas temporales Mantenimiento automático aplicado después y Último mantenimiento aplicado, se pueden ver en la Consola de administración de AWS o mediante el comando get-vpn-tunnel-replacement-status de la AWS CLI.

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 automático aplicado después, AWS realizará automáticamente la sustitución del punto de conexión del túnel poco después, como parte del ciclo de actualización de mantenimiento normal.

Habilitación del control del ciclo de vida del punto de conexión del túnel de AWS Site-to-Site VPN

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 con la Consola de administración de AWS o la 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 Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de 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. Seleccione Save changes (Guardar cambios).

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

Utilice el comando modify-vpn-tunnel-options para activar el control del ciclo de vida del punto de conexión 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 del punto de conexión del túnel durante la creación de una nueva conexión de VPN con la Consola de administración de AWS

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 (Conexiones de Site-to-Site VPN).
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 del punto de conexión del túnel durante la creación de una nueva conexión de VPN con la AWS CLI

Utilice el comando create-vpn-connection para activar el control del ciclo de vida del punto de conexión del túnel.

Verificación si el control del ciclo de vida del punto de conexión del túnel de AWS Site-to-Site VPN está habilitado

Puede comprobar si el control del ciclo de vida del punto de conexión del túnel está habilitado en un túnel de VPN existente mediante la Consola de administración de AWS o la CLI.

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

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

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de 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 comando describe-vpn-connections para comprobar si el control del ciclo de vida del punto de conexión del túnel está activado.

Comprobación de las actualizaciones del túnel de AWS Site-to-Site VPN 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 Consola de administración de AWS o la CLI. Comprobación de que una actualización del túnel de Site-to-Site VPN disponible no se descarga ni despliega automáticamente. 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 mediante la Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de 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 mediante la AWS CLI

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

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

Cuando haya una actualización de mantenimiento disponible, puede aceptarla mediante la Consola de administración de AWS o la CLI. Tiene la opción de elegir aceptar la actualización de mantenimiento del túnel de Site-to-Site VPN en el momento que más le convenga. Una vez que acepte la actualización de mantenimiento, se implementará.

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

Para aceptar una actualización de mantenimiento disponible con la Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de 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 con la AWS CLI

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

Desactivación del control del ciclo de vida del punto de conexión del túnel de AWS Site-to-Site VPN

Si ya no desea utilizar la característica de control del ciclo de vida del punto de conexión del túnel, puede desactivarla mediante la Consola de administración de AWS o la 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 característica sin utilizar la opción Omitir la sustitución del túnel, pero AWS implementará automáticamente las actualizaciones de mantenimiento pendientes disponibles al iniciar inmediatamente una sustitución del punto de conexión del túnel.

Para desactivar el control del ciclo de vida del punto de conexión del túnel con la Consola de administración de AWS

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación izquierdo, elija Conexiones de 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. Seleccione Save changes (Guardar cambios).

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

Utilice el comando modify-vpn-tunnel-options para desactivar el control del ciclo de vida del punto de conexión del túnel.

Opciones de gateway de cliente para su conexión de AWS Site-to-Site VPN

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` • 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 VPNOpciones de direccionamiento de .
La dirección IP de la interfaz externa del dispositivo de puerta de enlace de cliente.	La dirección IP debe ser estática y puede ser IPv4 o IPv6. Para direcciones IPv4: si su dispositivo de puerta de enlace de 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 en el puerto 500 (y en el puerto 4500, si se utiliza NAT transversal) tienen permiso para pasar entre la red y los puntos de conexión

Elemento	Descripción
	de AWS Site-to-Site VPN. Consulte Reglas de firewall para obtener más información. Para direcciones IPv6: la dirección debe ser una dirección IPv6 válida y enrutable por Internet. Las direcciones IPv6 solo son compatibles con conexiones de VPN en una puerta de enlace de tránsito o 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 entidad emisora de certificados subordinada que use 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. Cuando crea una gateway de cliente, puede configurarla para que utilice certificados privados de AWS Private Certificate Authority para autenticar Site-to-Site VPN. Cuando elige utilizar esta opción, crea un private certificate authority (CA) totalmente alojado en AWS para que la organización la utilice internamente. almacena y administra tanto el certificado de entidad de certificación raíz como la entidad de certificación subordina da Autoridad de certificación privada de AWS. Antes de crear la gateway de cliente, tiene que crear un certificado privado a partir de una CA subordinada mediante AWS Private Certifica te Authority y luego especifica el certificado al configurar la gateway de cliente. Para obtener información sobre la creación de un certifica do privado, consulte la sección de creación y administración de una CA privada en la Guía del usuario de AWS Private Certificate Authority.
(Opcional) Dispositivo.	Un nombre para el dispositivo de puerta de enlace de cliente asociado con esta puerta de enlace de cliente.

Opciones de puerta de enlace de cliente IPv6

Al crear una puerta de enlace de cliente con una dirección IPv6, tenga en cuenta lo siguiente:

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

```
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
```

Conexiones de AWS Site-to-Site VPN aceleradas

Si lo desea, puede acelerar la conexión de Site-to-Site VPN. Una conexión de Site-to-Site VPN acelerada (conexión VPN acelerada) utiliza AWS Global Accelerator para dirigir el tráfico de la red en las instalaciones a la ubicación de borde de AWS que esté más cerca del dispositivo de puerta de enlace de cliente. AWS Global Accelerator optimiza la ruta de red mediante el uso de la red global de AWS sin congestión para dirigir el tráfico al punto de conexión que proporcione el mejor rendimiento de la aplicación (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 por su cuenta con la consola o las API de AWS Global Accelerator.

Para obtener información acerca de las regiones de AWS que admiten conexiones VPN aceleradas, consulte Preguntas frecuentes acerca de AWS Site-to-Site VPN acelerada.

Habilitación de la aceleración

De forma predeterminada, cuando se crea una conexión de Site-to-Site VPN, la aceleración está desactivada. Si lo desea, puede activarla al realizar una nueva conexión de Site-to-Site VPN en

una gateway de tránsito. Para obtener más información y ver los pasos, consulte Creación de una conexión de puerta de enlace de tránsito de AWS Site-to-Site VPN.

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 en las conexiones de Site-to-Site VPN que están asociadas a una gateway de tránsito. Las gateway privadas virtuales no admiten conexiones de VPN aceleradas.
- No se puede utilizar una conexión de Site-to-Site VPN acelerada con una interfaz virtual pública de AWS Direct Connect.
- No se puede activar ni desactivar la aceleración para una conexión VPN de sitio a sitio existente. En su lugar, puede crear una nueva conexión VPN de sitio a sitio con aceleración activada o desactivada según sea necesario. A continuación, puede configurar el dispositivo de gateway de cliente para que utilice la nueva conexión de Site-to-Site VPN y elimine la anterior.
- 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.
- Es posible que las conexiones de Site-to-Site VPN que utilizan la autenticación basada en certificados no puedan utilizarse con AWS Global Accelerator debido a la compatibilidad limitada de Global Accelerator con la fragmentación de paquetes. Para obtener más información, consulte Funcionamiento de 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 VPNOpciones de direccionamiento de

AWS recomienda anunciar rutas de BGP específicas para influir en las decisiones de enrutamiento de la gateway 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.

Cuando cree una conexión de 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 gateway de cliente admite el protocolo de Número de sistema autónomo (ASN), especifique el direccionamiento dinámico al configurar la conexión de Site-to-Site VPN. Si el dispositivo de gateway de cliente no admite BGP, especifique un enrutamiento estático.

Si utiliza un dispositivo que admite publicidad de ASN, no será necesario especificar ninguna ruta estática en la conexión de Site-to-Site VPN, ya que el dispositivo utiliza ASN para anunciar sus rutas a la gateway 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 gateway de cliente para enrutar el tráfico desde la red local a la conexión de Site-to-Site VPN. La configuración depende del fabricante y el modelo del dispositivo. Para obtener más información, consulte dispositivos de puerta de enlace de cliente de AWS Site-to-Site VPN.

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 de una conexión Site-to-Site VPN o de una conexión Direct Connect se solapan con la ruta local para su VPC, la ruta local es la más preferida aunque las rutas propagadas sean más específicas.
- Si las rutas propagadas desde una conexión de Site-to-Site VPN o Direct Connect tienen el mismo bloque de CIDR de destino que otras rutas estáticas (cuando no sea posible aplicar la coincidencia de prefijo más largo), se dará prioridad a las rutas estáticas cuyos objetivos sean puertas de enlace de Internet, puertas de enlace privadas virtuales, interfaces de red, ID de instancia, una conexión de emparejamiento de VPC, puertas de enlace NAT, transit gateway o puntos de conexión de VPC de una 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 puerta de enlaces privadas virtuales no admiten el 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 VPN en puertas de enlace privadas virtuales y puertas de enlace 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 de BGP desde una conexión de Direct Connect

  Las rutas de agujeros negros no se propagan a una puerta de enlace de cliente de Site-to-Site VPN mediante BGP.
- Rutas estáticas agregadas manualmente para una conexión de Site-to-Site VPN
- Rutas propagadas por ASN desde una conexión de Site-to-Site VPN
- En los prefijos que coinciden donde cada conexión de Site-to-Site VPN utiliza ASN, se compara la ruta AS PATH y se elige el prefijo con la ruta AS PATH más corta.

> **Note**
>
> AWS recomienda encarecidamente utilizar dispositivos de puerta de enlace de clientes que admiten 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. De esta forma, podrá asegurarse de que el valor multi-exit discriminator (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 las rutas AS PATH tengan la misma longitud y si el primer AS de AS_SEQUENCE es el mismo en varias rutas, se comparan los multi-exit discriminators (MED). 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 de 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 VPN en puertas de enlace privadas virtuales y puertas de enlace de tránsito.

En una gateway privada virtual, se seleccionará un solo túnel entre todas las conexiones de Site-to-Site VPN de la gateway. Para utilizar varios túneles, le recomendamos que considere las rutas múltiples de igual costo (ECMP), que se admiten en conexiones de Site-to-Site VPN de las gateways de tránsito. Para obtener más información, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC. ECMP no es puede utilizarse con las conexiones de Site-to-Site VPN de una gateway privada virtual.

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

En las conexiones de Site-to-Site VPN que utilizan un direccionamiento estático, el túnel principal se puede identificar a través de estadísticas de tráfico o métricas.

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

Una conexión de Site-to-Site VPN consta de dos túneles de VPN entre un dispositivo de gateway de cliente y una gateway privada virtual o una gateway de tránsito. Recomendamos configurar ambos túneles para la redundancia. Cada cierto tiempo, AWS también lleva a cabo un mantenimiento rutinario en la conexión VPN, lo que podría desactivar uno de los dos túneles de la conexión VPN durante un breve periodo. 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).

Tráfico de IPv4 e IPv6 en AWS Site-to-Site VPN

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

Si activa IPv6 en los túneles de VPN de la conexión de Site-to-Site VPN, cada túnel tendrá dos bloques de CIDR. Uno es un bloque CIDR IPv4 de tamaño /30 y el otro es un bloque CIDR IPv6 de tamaño /126.

Compatibilidad con IPv4 e IPv6

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

- Túnel externo IPv4 con paquetes internos de IPv4: capacidad básica de VPN IPv4 compatible con puertas de enlace privadas virtuales, puertas de enlace de tránsito y WAN en la nube.
- Túnel externo de IPv4 con paquetes internos de IPv6: permite transporte y aplicaciones de IPv6 en el túnel de VPN. Compatible con las puertas de enlace de tránsito y WAN en la nube. No es compatible con las puertas de enlace privadas virtuales.
- Túnel externo de IPv6 con paquetes internos de IPv6: permite la migración completa de IPv6 con direcciones IPv6 tanto para las IP de túnel externo como para las IP de los paquetes internos. Compatible tanto con las puertas de enlace de tránsito como con WAN en la nube.
- Túnel externo IPv6 con paquetes internos de IPv4: permite el direccionamiento del túnel externo de IPv6 y, al mismo tiempo, admite aplicaciones IPv4 antiguas en el túnel. Compatible tanto con las puertas de enlace de tránsito como con WAN en la nube.

Se aplican las siguientes reglas:

- Las direcciones IPv6 de las IP de túnel externo solo se admiten en las conexiones de Site-to-Site VPN que terminan en una puerta de enlace de tránsito o en WAN en la nube. Las conexiones de Site-to-Site VPN en una puerta de enlace privada virtual no admiten IPv6 para IP de túnel externo.
- Cuando utilice IPv6 para IP de túneles externos, debe asignar direcciones IPv6 tanto en el extremo de AWS de la conexión de VPN como en la puerta de enlace de cliente para ambos túneles de VPN.
- La compatibilidad con IPv6 no se puede activar en una conexión de Site-to-Site VPN existente. Debe eliminar la conexión existente y crear una nueva.
- Una conexión de Site-to-Site VPN no admite el tráfico de IPv4 e IPv6 simultáneamente. Los paquetes encapsulados internos pueden ser IPv6 o IPv4, pero no ambos. Necesita conexiones de Site-to-Site VPN independientes para transportar los paquetes IPv4 e IPv6.
- Las VPN IP privadas no admiten direcciones IPv6 para IP de túnel externo. Utilizan direcciones RFC 1918 o CGNAT. Para obtener más información sobre RFC 1918, consulte RFC 1918: asignación de direcciones para internets privadas.

- Las VPN IPv6 admiten el mismo rendimiento (Gbps y PPS), MTU y límites de ruta que las VPN IPv4.
- El cifrado IPsec y el intercambio de claves funcionan de la misma manera para VPN IPv4 e IPv6.

Para obtener más información sobre la creación de una conexión de VPN que admita IPv6, consulte Creación de una conexión de VPN en Introducción a Site-to-Site VPN.

Empiece a utilizar AWS Site-to-Site VPN

Utilice el procedimiento siguiente para configurar una conexión de AWS Site-to-Site VPN. 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 especifica “No asociada”, podrá elegir el tipo de puerta de enlace de destino más adelante o podrá utilizarla como asociación 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 de VPN para AWS Cloud WAN, consulte Creación 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).
Gateway de cliente	Para crear el recurso de gateway de cliente 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 para el lado de AWS de una 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 la conexión de AWS Site-to-Site VPN.

Paso 1: Crear una puerta de enlace de cliente

Una gateway de cliente proporciona información a AWS acerca de su dispositivo de gateway de cliente o aplicación de software. Para obtener más información, consulte Puerta de enlace de cliente.

Si tiene previsto usar un certificado privado para autenticar la VPN, cree un certificado privado a partir de una CA subordinada mediante 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. En Tipo de dirección IP, elija una de las siguientes opciones:
   - IPv4: (predeterminado) especifique una dirección IPv4 para el dispositivo de puerta de enlace de cliente.

- IPv6: especifique una dirección IPv6 para el dispositivo de puerta de enlace de cliente. Esta opción es necesaria al crear una conexión de VPN con IP de túnel externo de IPv6.

7. En Dirección IP, introduzca la dirección IP direccionable de Internet estática del dispositivo de puerta de enlace 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 consulta de Amazon EC2)
- create-customer-gateway (AWS CLI)

  Ejemplo de creación de una puerta de enlace de cliente IPv6:

```
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 de VPN entre la VPC y la red en las instalaciones, debe crear una gateway de destino en el lado de AWS 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. En VPC disponibles, elija su VPC y después elija Asociar a la VPC.

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

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

Crear una gateway 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 desactivar la propagación de rutas para que la tabla de enrutamiento propague automáticamente las rutas de 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

Destination (Destino), agregue la ruta estática que se utiliza en la conexión de 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 consulta de Amazon EC2)
- 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 consulta de Amazon EC2)
- 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, elija 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, elija Conexiones de 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 direccionamiento en función de si el dispositivo de puerta de enlace de cliente admite el protocolo de puerta de enlace 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). 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 compartidas previamente:

   - Estándar: la clave compartida previamente se guarda directamente en el servicio Site-to-Site VPN.
   - Secrets Manager: la clave compartida previamente se almacena mediante AWS Secrets Manager. Para obtener más información acerca de Secrets Manager, consulte Características de seguridad mejoradas con Secrets Manager.
8. Si la puerta de enlace de destino es la puerta de enlace de tránsito, en Túnel dentro de la versión IP, especifique si los túneles de la VPN admiten tráfico IPv4 o IPv6. El tráfico IPv6 solo es compatible con conexiones VPN en una gateway de tránsito.
9. Si especificó IPv4 para Túnel dentro de la versión IP, puede especificar opcionalmente los intervalos CIDR de IPv4 para la puerta de enlace de cliente y los lados de AWS que tienen permiso para comunicarse a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0`.

   Si especificó IPv6 para Túnel dentro de la versión IP, puede especificar opcionalmente los intervalos CIDR de IPv6 para la puerta de enlace de cliente y los lados de AWS que tienen permiso para comunicarse a través de los túneles de VPN. El valor predeterminado para ambos rangos es `::/0`.
10. En Tipo de dirección IP externa, elija una de las siguientes opciones:

    - PublicIpv4: (predeterminado) utilice direcciones IPv4 para las IP de túnel externo.

- IPv6: utilice direcciones IPv6 para las IP de túnel externo. Esta opción solo está disponible para conexiones de VPN en una puerta de enlace de tránsito o de WAN en la nube.

11. (Opcional) En Opciones de túnel, puede especificar la siguiente información para cada túnel:

    - Un bloque CIDR IPv4 de tamaño /30 desde el rango `169.254.0.0/16` para las direcciones IPv4 de túnel interior.
    - Si especificó IPv6 en Túnel dentro de la versión IP, un bloque de CIDR IPv6 /126 del intervalo `fd00::/8` para las direcciones IPv6 del túnel interior.
    - La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: 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 consulta de Amazon EC2)
- create-vpn-connection (AWS CLI)

  Ejemplo de creación de una conexión de VPN con IP de túnel externo IPv6 e IP de túnel interno IPv6:

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

  Ejemplo de creación de una conexión de VPN con IP de túnel externo IPv6 e IP de túnel interno IPv4:

```
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 de Site-to-Site VPN de AES128, SHA1 y Diffie-Hellman grupo 2 en la mayoría de las regiones de AWS, y AES128, SHA2 y Diffie-Hellman grupo 14 en las regiones GovCloud de AWS. También especifica claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos Diffie-Hellman, los certificados privados y el tráfico IPv6.
>
> Hemos agregado la compatibilidad con IKEv2 en los archivos de configuración para muchos dispositivos populares de gateway de cliente y continuaremos agregando archivos adicionales con el tiempo. Para obtener una lista de archivos de configuración con compatibilidad con IKEv2, consulte dispositivos de puerta de enlace de cliente de AWS Site-to-Site VPN.

Permisos

Para cargar correctamente la pantalla de configuración de descarga desde la Consola de administración de AWS, debe asegurarse de que su rol de IAM o usuario tienen permiso para las siguientes API de Amazon EC2: `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, elija Conexiones de 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 (API de Amazon EC2)
- GetVPNConnectionDevicesAmplipleConfiguration (API de consulta de Amazon EC2)
- get-vpn-connection-device-types (AWS CLI)
- get-vpn-connection-device-sample-configuration (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 dispositivos de puerta de enlace de cliente de AWS Site-to-Site VPN.

escenarios arquitectónicos de AWS Site-to-Site VPN

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 de VPN adicionales desde la ubicación de las instalaciones a otras VPC con el mismo dispositivo de gateway de cliente. Puede reutilizar la misma dirección IP de gateway de cliente para cada una de estas conexiones de VPN.

Varios dispositivos de gateway de cliente a una única gateway privada virtual (Site-to-Site 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 AWS VPN CloudHub. Para obtener más información, consulte Comunicación segura entre conexiones de AWS Site-to-Site VPN 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 Conexiones de AWS Site-to-Site VPN 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.

A continuación se muestran algunas arquitecturas comunes de Site-to-Site VPN:

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

Ejemplos de conexión de VPN única y múltiple de AWS Site-to-Site VPN

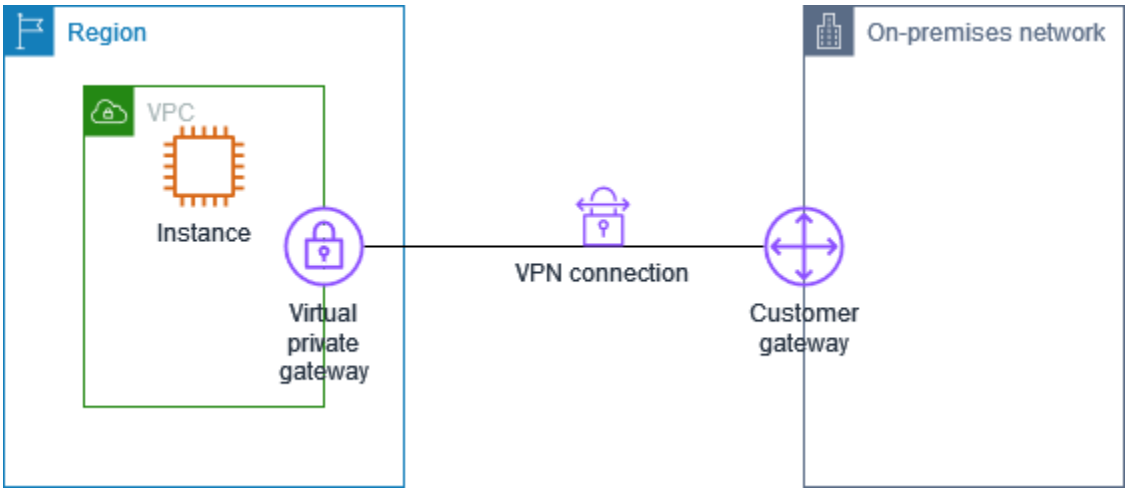
En los diagramas siguientes, se muestra una conexión única de Site-to-Site VPN y otra múltiple.

Ejemplos

- Conexión única de Site-to-Site VPN
- Conexión de Site-to-Site VPN con una gateway de tránsito
- Conexiones múltiples de Site-to-Site VPN
- Conexiones múltiples de Site-to-Site VPN con una gateway de tránsito
- Conexión de Site-to-Site VPN con Direct Connect
- Conexión de Site-to-Site VPN de IP privada con Direct Connect

Conexión única de Site-to-Site VPN

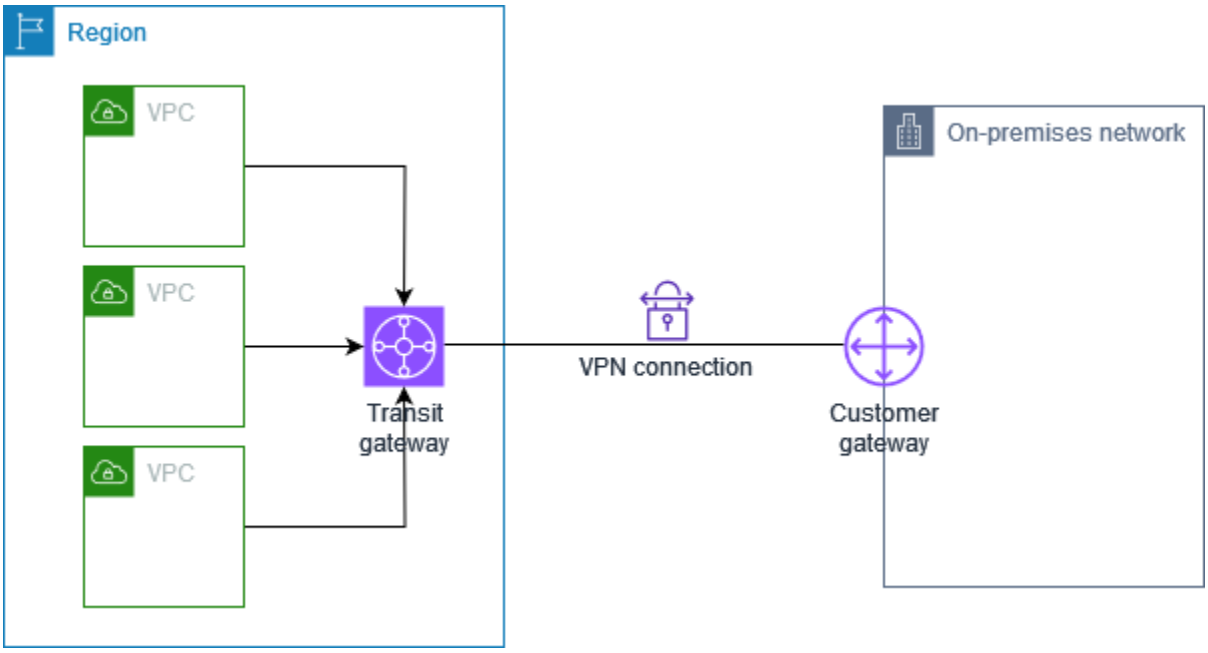
La VPC dispone de una puerta de enlace privada virtual asociada y su red en las instalaciones (remota) incluye un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada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



Si desea ver los pasos necesarios para configurar este escenario, consulte Empiece a utilizar AWS Site-to-Site VPN.

Conexión de Site-to-Site VPN con una gateway de tránsito

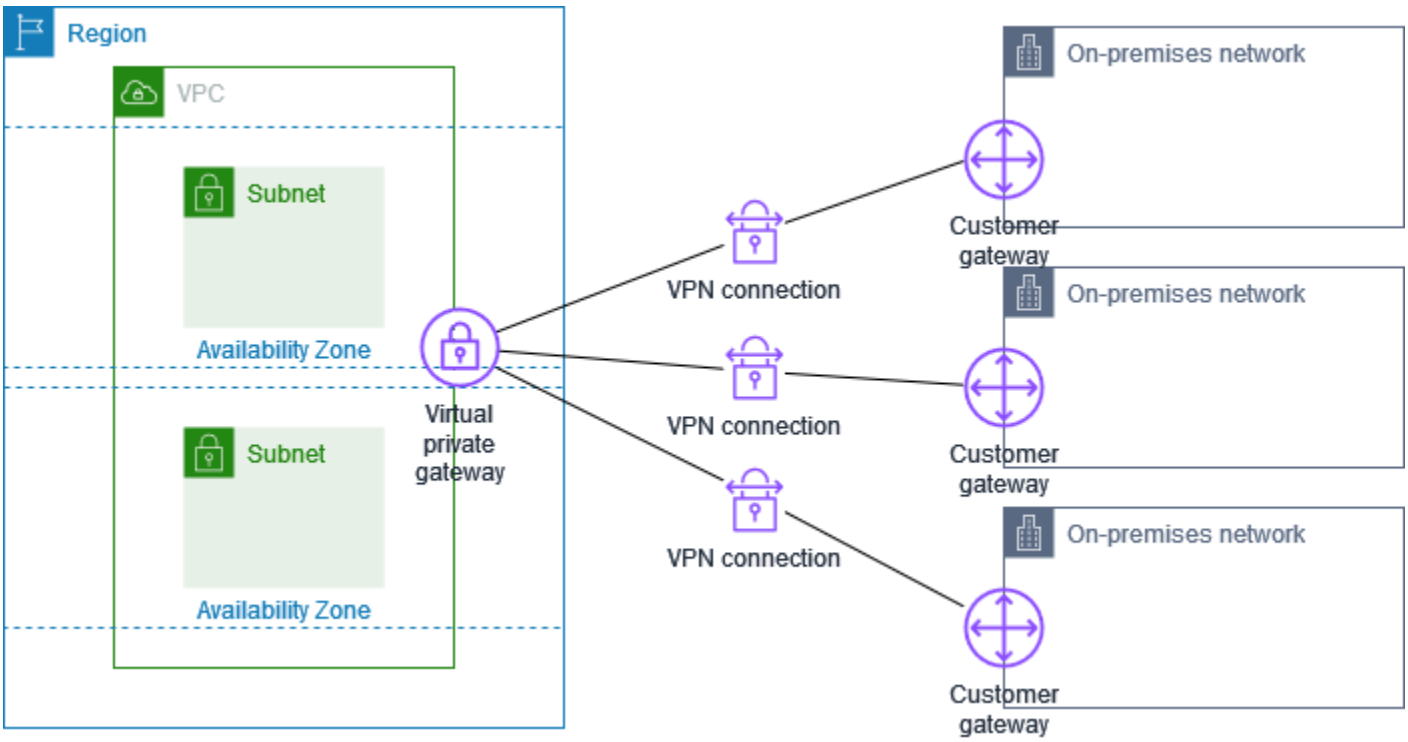
La VPC dispone de una puerta de enlace de tránsito asociada y la red en las instalaciones (remota) contiene un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión de VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada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



Si desea ver los pasos necesarios para configurar este escenario, consulte Empiece a utilizar AWS Site-to-Site VPN.

Conexiones múltiples de Site-to-Site VPN

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

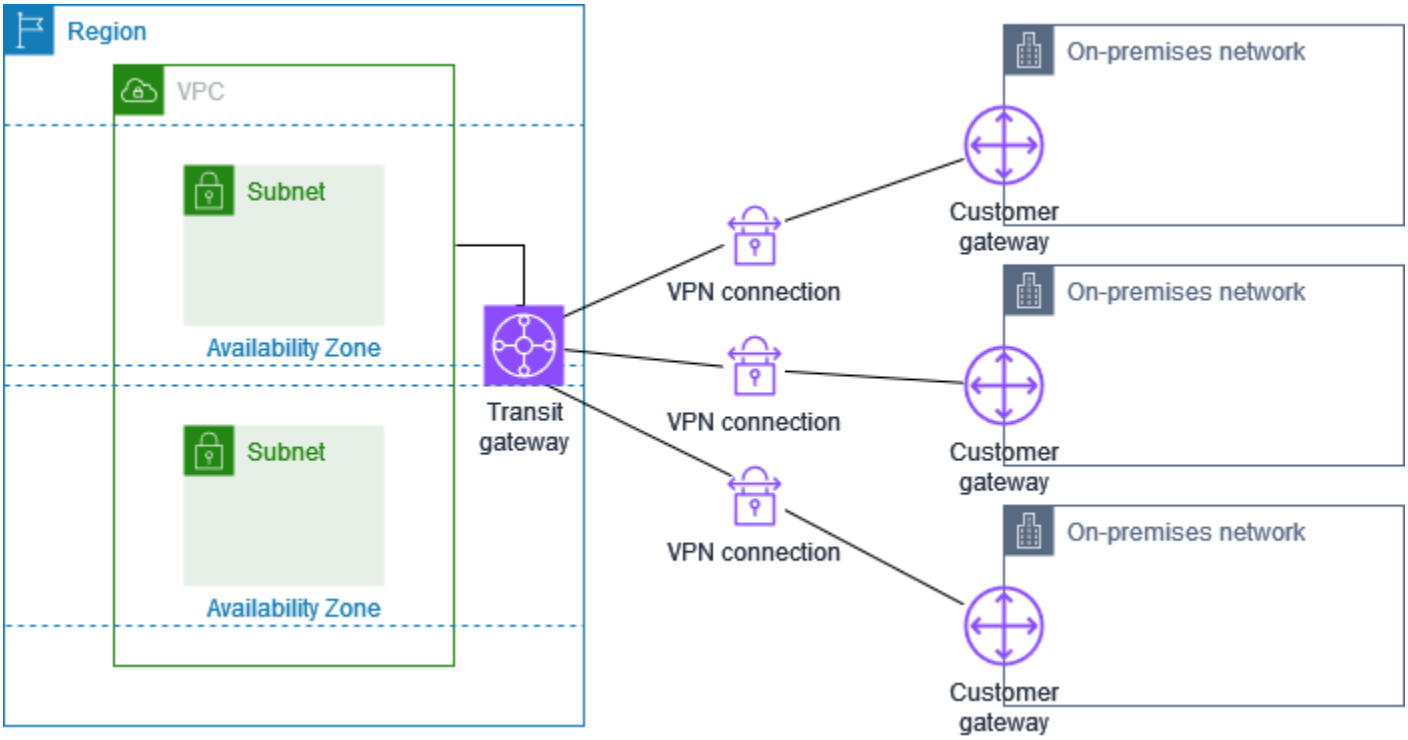


Si crea varias conexiones de Site-to-Site VPN con una única VPC, puede configurar una segunda gateway de cliente para crear una conexión redundante con la misma ubicación externa. Para obtener más información, consulte Conexiones de AWS Site-to-Site VPN redundantes para conmutación por error.

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

Conexiones múltiples de Site-to-Site VPN con una gateway de tránsito

La VPC tiene una gateway de tránsito conectada y hay varias conexiones de Site-to-Site VPN con diversas 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.

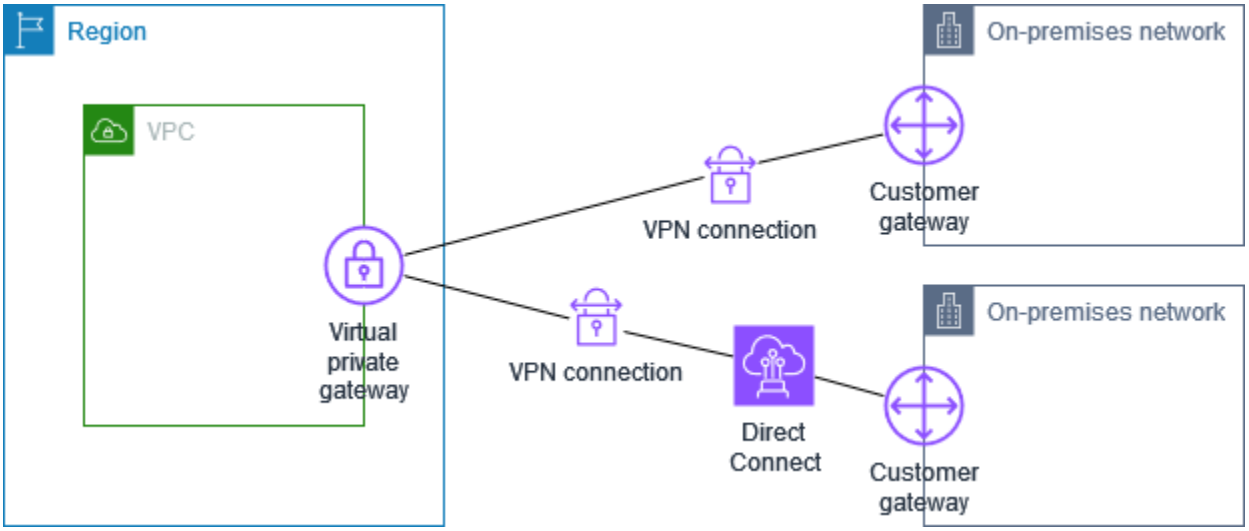


Si crea varias conexiones de Site-to-Site VPN con una única gateway de tránsito, puede configurar una segunda gateway de cliente para crear una conexión redundante con la misma ubicación externa.

También puede utilizar esta situación para crear conexiones de Site-to-Site VPN con varias ubicaciones geográficas y proporcionar una comunicación segura entre sitios.

Conexión de Site-to-Site VPN con Direct Connect

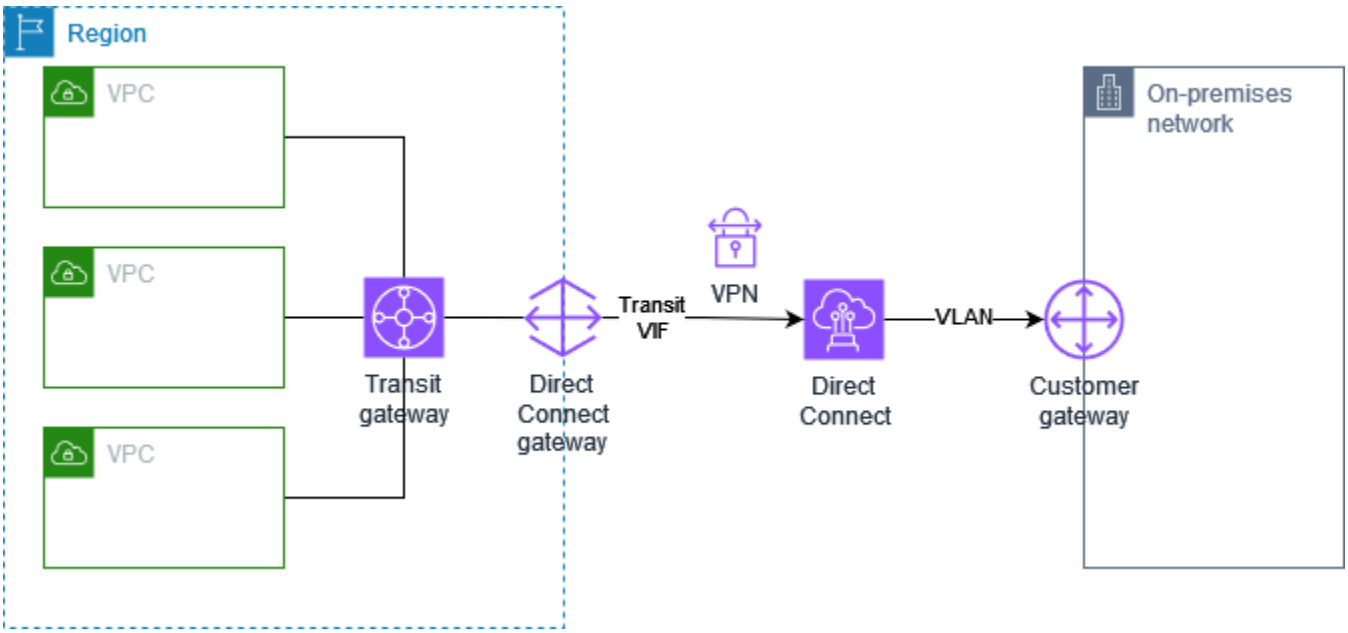
La VPC tiene una gateway privada virtual conectada y se conecta a su red en las instalaciones (remota) a través de AWS Direct Connect. Puede configurar una interfaz virtual pública de Direct Connect para establecer una conexión de red dedicada entre la red y los recursos públicos de AWS a través de una puerta de enlace privada virtual. Configure el enrutamiento para que cualquier tráfico de la VPC vinculada a la red se dirija a la puerta de enlace privada virtual y a la conexión de Direct Connect.



Cuando tanto Direct Connect como la conexión de VPN están configurados en la misma puerta de enlace privada virtual, agregar o quitar objetos podría provocar que la puerta de enlace privada virtual entre en el estado "conectando". Esto indica que se está realizando un cambio en el enrutamiento interno que cambiará entre 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 de Site-to-Site VPN de IP privada con Direct Connect

Con una VPN de sitio a sitio de IP privada puede cifrar el tráfico de Direct Connect entre su red en las instalaciones y AWS sin usar direcciones IP públicas. La VPN de IP privada a través de Direct Connect garantiza que el tráfico entre AWS y las redes en las instalaciones es seguro y privado, lo que permite a los clientes cumplir los mandatos normativos y de seguridad.



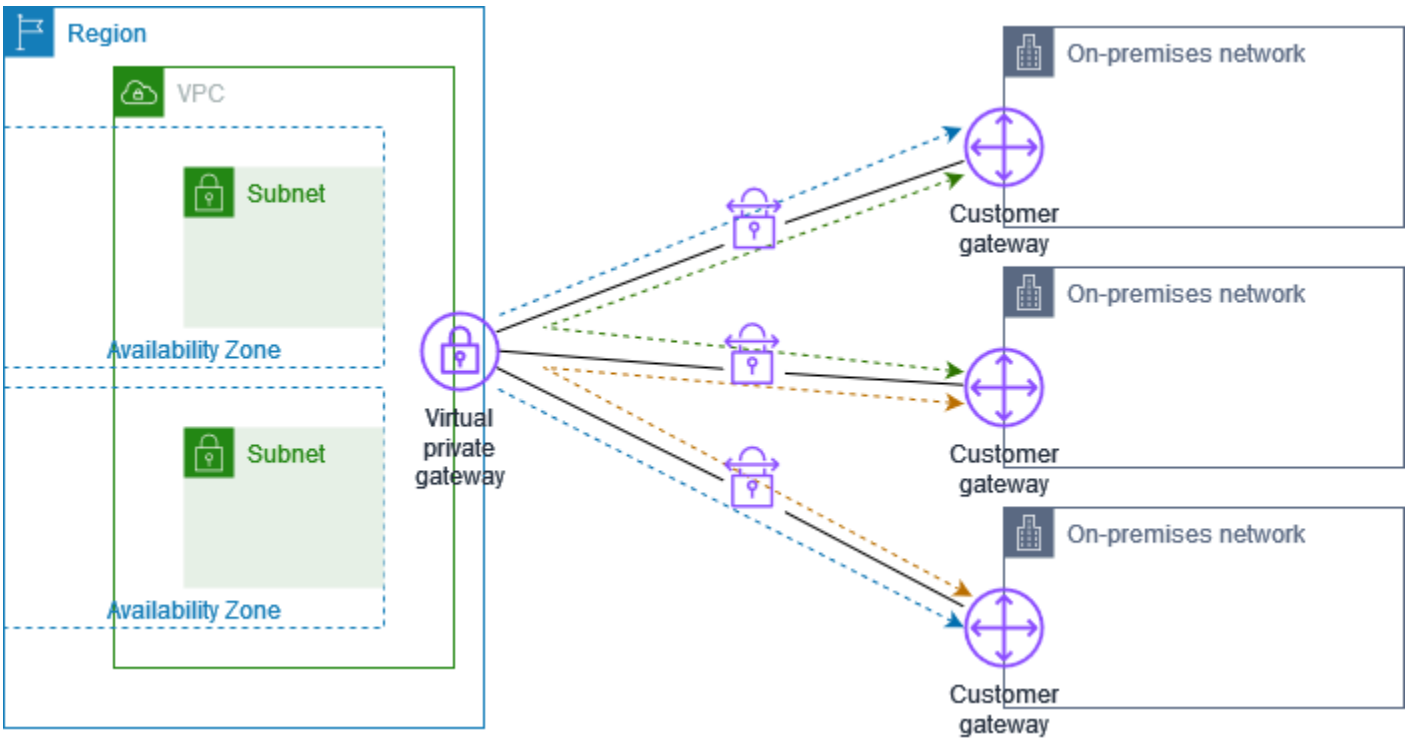
Para obtener más información, consulte la siguiente entrada de blog: Introducing AWS Site-to-Site VPN Private IP VPNs (Introducción a las VPN con IP privadas de AWS Site-to-Site VPN VPN).

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

Si tiene varias conexiones de AWS Site-to-Site VPN, puede proporcionar seguridad en la comunicación entre sitios gracias a AWS VPN CloudHub. Esto permite que los sitios puedan comunicarse entre sí y no solo con los recursos de la VPC. VPN CloudHub funciona con un modelo radial sencillo que puede utilizar con o sin VPC. Este diseño es perfecto si tiene varias sucursales y conexiones a Internet existentes y desea implementar un sistema radial cómodo y potencialmente de bajo coste para la conectividad principal o auxiliar entre estos sitios.

Descripción general

En el siguiente diagrama se muestra la arquitectura de VPN CloudHub. 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 de Site-to-Site VPN con direccionamiento dinámico entre cada gateway de cliente y la gateway 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 realiza utilizando las instrucciones de red de los archivos de configuración de VPN de la conexión de 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 las conexiones de Direct Connect a la puerta de enlace privada virtual también pueden ser parte de AWS VPN CloudHub. Por ejemplo, su sede corporativa de Nueva York puede tener una conexión de Direct Connect a la VPC y sus sucursales pueden utilizar las conexiones de Site-to-Site VPN a la VPC. De este modo, las sucursales de Los Ángeles y Miami podrán enviar y recibir datos a la sede corporativa y entre ellas mismas gracias a AWS VPN CloudHub.

Precios

Para utilizar AWS VPN CloudHub, debe pagar las tarifas de conexión habituales de Site-to-Site VPN para Amazon VPC. De este modo, se le facturará las tasas de conexión por cada hora que cada VPN permanezca conectada a la gateway privada virtual. Al enviar datos de un sitio a otro mediante AWS VPN CloudHub, no incurrirá en ningún costo para el envío de datos desde su sitio a la puerta de enlace privada virtual. Solo pagará tasas de transferencia de datos de AWS estándar de los datos que se reenvíen desde la puerta de enlace privada virtual al punto de conexión.

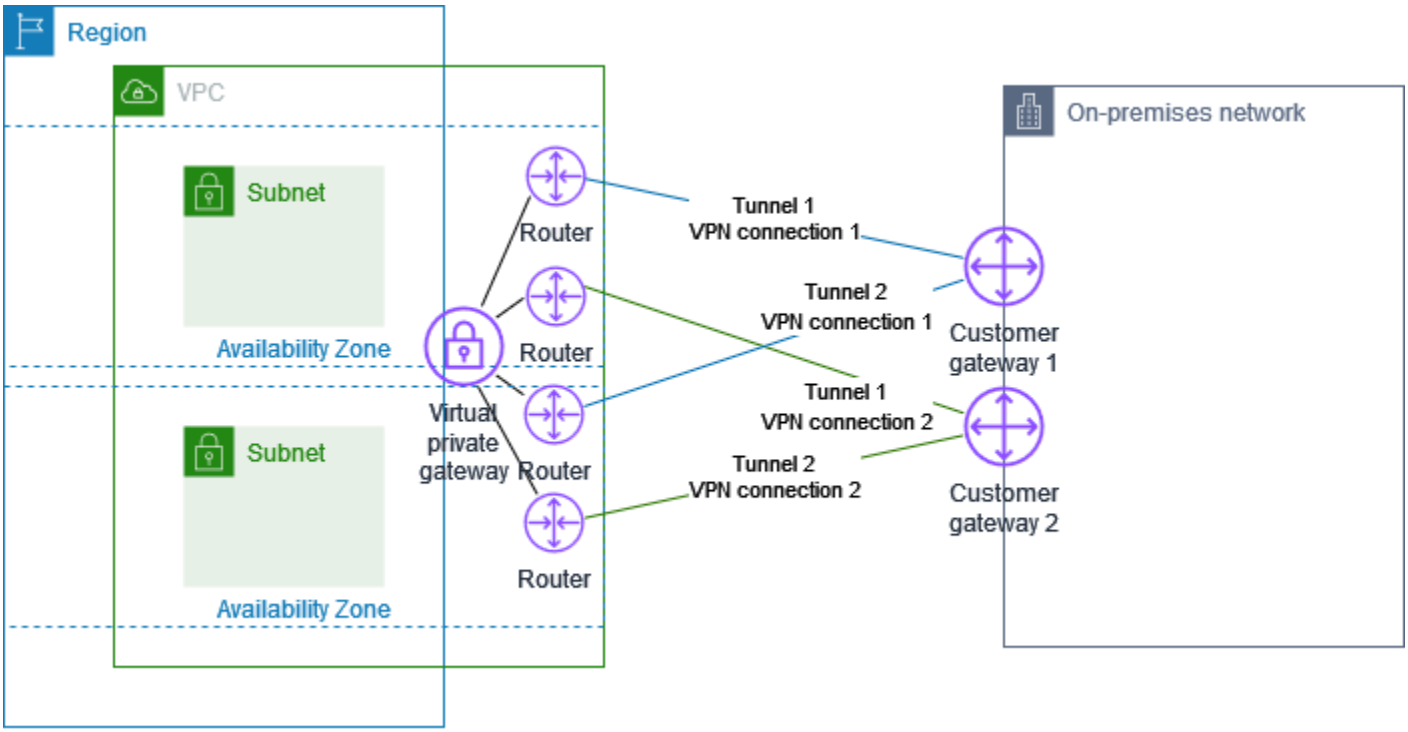
Por ejemplo, si tiene un sitio en Los Ángeles y otro sitio en Nueva York y ambos sitios tienen una conexión de Site-to-Site VPN con la gateway privada virtual, se le aplicará la tarifa por hora por cada conexión de Site-to-Site VPN (por tanto, si la tarifa fuera de 0,05 USD por hora, equivaldría a un total de 0,10 USD por hora). También se le aplicarán las tarifas estándar de transferencia de datos de AWS para todos los datos que envíe de Los Ángeles a Nueva York (y viceversa) y que atraviesen cada conexión de Site-to-Site VPN. El tráfico de red que se envía a través de la conexión de Site-to-Site VPN a la puerta de enlace privada virtual es gratuito, pero el tráfico de red que se envía a través de la conexión de Site-to-Site VPN desde la puerta de enlace privada virtual al punto de conexión se factura según la tarifa de transferencia de datos estándar de AWS.

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

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

Para protegerse frente a la pérdida de conectividad que se produciría si su dispositivo de puerta de enlace de cliente dejara de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN con la VPC y la puerta de enlace privada virtual utilizando otro 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 otra conexión de Site-to-Site VPN utilizando la misma gateway privada virtual y creando una nueva gateway de cliente. La dirección IP de la gateway de cliente de la segunda conexión de Site-to-Site VPN debe estar disponible públicamente.
- 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 de Site-to-Site VPN de direccionamiento dinámico utilizan el protocolo de Número de sistema autónomo (ASN) para intercambiar la información de direccionamiento entre las gateways de cliente y las gateways privadas virtuales. En las conexiones de Site-to-Site VPN con direccionamiento estático, es necesario que las rutas estáticas de la red remota se escriban en su lado de la gateway de 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

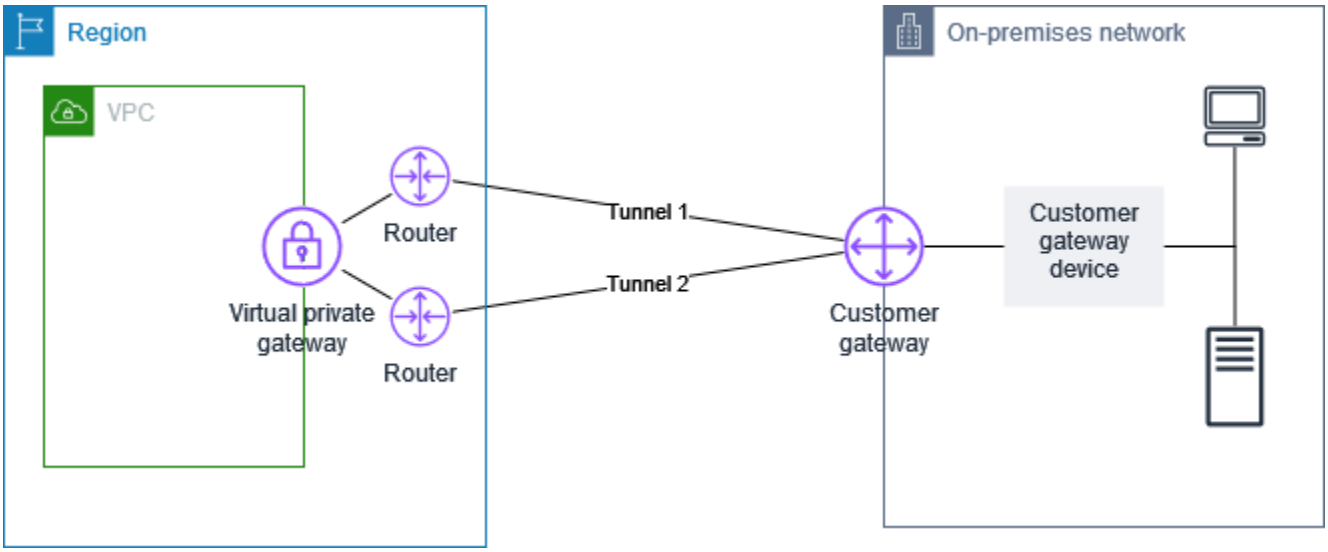
disponible) y seleccionar una ruta alternativa. La configuración exacta dependerá de la arquitectura de su red.

Para obtener más información acerca de cómo crear y configurar una gateway de cliente y una conexión de Site-to-Site VPN, consulte Empiece a utilizar AWS Site-to-Site VPN.

dispositivos de puerta de enlace de cliente de AWS Site-to-Site VPN

Un dispositivo de gateway de cliente es un dispositivo físico o de software que usted posee o administra en la red local (en su extremo de una conexión de Site-to-Site VPN). Usted o el administrador de red tienen que configurar el dispositivo para que funcione con la conexión de 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 error del dispositivo en AWS, su conexión de VPN cambiará automáticamente al segundo túnel para que su acceso no se vea interrumpido. Cada cierto tiempo, AWS también lleva a cabo un mantenimiento rutinario en la conexión de VPN, lo que podría desactivar uno de los dos túneles de la conexión de VPN durante un breve periodo. Para obtener más información, consulte reemplazos de los puntos de conexión de un túnel de AWS Site-to-Site VPN. 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 Empiece a utilizar AWS Site-to-Site VPN. Durante este proceso, crea un recurso de gateway de cliente en AWS, que proporciona información a AWS sobre el dispositivo como, por ejemplo, su dirección IP pública. Para obtener más información, consulte Opciones de gateway de cliente para su conexión de AWS Site-

to-Site VPN. El recurso de gateway de cliente en AWS no configura ni crea el dispositivo de gateway de cliente. Debe configurar el dispositivo usted mismo.

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

Requisitos para un dispositivo de puerta de enlace de cliente de AWS Site-to-Site VPN

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

Si tiene un dispositivo que no está en la lista anterior de dispositivos compatibles, consulte la sección siguiente, en la que se describen los requisitos que debe cumplir el dispositivo para establecer una conexión con 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). Necesaria para intercambiar claves utilizadas para establecer la asociación de seguridad de IPsec.
IPsec	Asociación de seguridad IPsec. 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 de IKE, una asociación de seguridad de IPsec y un intercambio de tráfico BGP. La

limitación es de una única pareja de asociación de seguridad (SA) por túnel (un entrante y uno saliente) y, por lo tanto, dos únicas parejas de SA en total para los dos túneles (cuatro SA). Algunos dispositivos utilizan una VPN basada en políticas y crean tantas SA como entradas de ACL. 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. Puede configurar la conexión de VPN para iniciar la negociación de IKE desde el lado de la conexión AWS. Para obtener más información, consulte AWS Site-to-Site VPNOpciones de inicio de túnel de .

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 de IKE se establece primero entre la gateway privada virtual y el dispositivo de gateway de cliente mediante una clave compartid a previamente o un certificado privado que usen 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 de VPN en AWS, puede especificar su propia clave previamente compartida para cada túnel o puede dejar que AWS genere una automáticamente. Como opción alternativa, puede especificar el certificado privado mediante AWS Private Certificate Authority para utilizarlo para el dispositivo de gateway de cliente. Para obtener más información sobre la configuración de túneles de VPN, consulte Opciones de túnel para la conexión de AWS Site-to-Site VPN.

Requisito	RFC	Comentarios
		Las siguientes versiones son compatibles: IKEv1 e IKEv2. El modo principal solo se admite con IKEv1. 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.
Establecimiento de asociaciones de seguridad de IPsec en modo de túnel IPsec	RFC 4301	Mediante la clave efímera de IKE, se establecen las claves entre la gateway privada virtual y el dispositivo de gateway de cliente para crear una asociación de seguridad (SA) de IPsec. El tráfico entre las gateways se cifra y se descifra mediante esta SA. IKE cambia automáticamente las claves efímeras utilizadas para cifrar el tráfico dentro de la SA de IPsec de forma periódica 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 entre las asociaciones de seguridad de IKE y de IPsec.
Uso de la función de hash SHA-1 o SHA-2 (256)	RFC 2404	Esta función de hash se utiliza para autenticar asociaciones de seguridad de IKE y de IPsec.
Uso de la confidenc ialidad 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 de VPN enrutadas dinámicamente) Uso de la detección de pares muertos de 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, se utiliza el túnel IPsec alternativo, si es posible.
(Conexiones de VPN enrutadas dinámicamente) Vincular el túnel a la interfaz lógica (VPN basada en rutas) Tunnel	Ninguno	El dispositivo debe poder vincular el túnel IPSec 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 mediante la asociación de seguridad de IPsec. BGP es necesario para que ambas gateways intercambien los prefijos IP, a los que se obtiene acceso mediante la SA de IPsec.

Una conexión de VPN de AWS no es compatible con la detección de la ruta 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 de cliente de AWS Site-to-Site VPN.

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

Uso de IKEv2

Recomendamos encarecidamente el uso de IKEv2 para la conexión de Site-to-Site VPN. IKEv2 es un protocolo más simple, robusto y seguro que IKEv1. Solo debe usar IKEv1 si el dispositivo de puerta de enlace de cliente no admite 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 la conexión de 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 de cliente para fragmentar los paquetes antes de cifrarlos. Luego, Site-to-Site VPN volverá a ensamblar los paquetes fragmentados antes de reenviarlos al siguiente destino, a fin de lograr un mayor flujo de paquetes por segundo a través de la red de AWS. Consulte RFC 4459 para obtener más información.

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

Dado que Site-to-Site VPN volverá a ensamblar los paquetes fragmentados recibidos desde el dispositivo de puerta de enlace de cliente antes de reenviarlos al siguiente destino, no olvide que es posible que haya que tener en cuenta el tamaño del paquete o MTU para las redes de destino a las que estos paquetes se reenvíen a continuación, por ejemplo Direct Connect o con determinados protocolos, como Radius.

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

Los paquetes TCP suelen ser el tipo más común de paquetes en los túneles IPsec. Site-to-Site VPN admite una unidad máxima de transmisión (MTU) de 1446 bytes y un tamaño máximo de segmento (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 en IPv4)
AES-GCM-16	N/A	disabled	1446	1406	1386
AES-GCM-16	N/A	enabled	1438	1398	1378
AES-CBC	SHA1, SHA2-256	disabled	1438	1398	1378
AES-CBC	SHA1, SHA2-256	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.

Desactivación de los ID únicos de IKE

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 de cliente de AWS Site-to-Site VPN

Debe tener una dirección IP estática para utilizarla como punto de conexión de los túneles IPsec que conectan su dispositivo de puerta de enlace de cliente con los puntos de conexión de AWS Site-to-Site VPN. Si existe un firewall entre AWS y su dispositivo de puerta de enlace de cliente, las reglas de las tablas siguientes deben estar aplicadas para establecer los túneles IPsec. Las direcciones IP en AWS estará 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 paquetes IPsec que contienen el tráfico de red cifrado.

> **Note**
>
> Si utiliza NAT transversal (NAT-T) en el dispositivo, asegúrese de que el tráfico UDP en el puerto 4500 también puede pasar entre la red y los puntos de conexión de 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 de cliente de AWS Site-to-Site VPN

Después de crear la conexión de VPN, también tiene la opción de descargar un proporcionado por AWS el archivo de configuración de ejemplo desde la consola de Amazon VPC o mediante la API de EC2. 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 de configuración de ejemplo proporcionado por AWS contiene información específica de su conexión de VPN que puede usar para configurar su dispositivo de gateway de cliente. 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 con la configuración de conexión de Site-to-Site VPN completamente. Especifica los requisitos mínimos para una conexión Site-to-Site VPN de AES128, SHA1 y Diffie-Hellman grupo 2 en la mayoría de Regiones AWS, y AES128, SHA2 y Diffie-Hellman grupo 14 en las Regiones AWS de GovCloud. También especifica claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos Diffie-Hellman, los certificados privados y el tráfico IPv6.

> **Note**
>
> Estos archivos de configuración específicos del dispositivo son proporcionados por AWS en la medida de lo posible. Si bien han sido probados por AWS, esta prueba es limitada. Si experimenta un problema con los archivos de configuración, es posible que deba contactar al proveedor específico para obtener asistencia adicional.

La tabla siguiente contiene una lista de dispositivos que tienen un archivo de configuración de ejemplo disponible para descargar que se ha actualizado para ser compatible con IKEv2. Hemos agregado la compatibilidad con IKEv2 en los archivos de configuración para muchos dispositivos populares de gateway de cliente y continuaremos agregando archivos adicionales con el 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.	AMI CSrV	IOS 12.4+

Proveedor	Plataforma	Software
Fortinet	Serie Fortigate 40+	ForTIOS 6.4.4+ (GUI)
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 de cliente de AWS Site-to-Site VPN

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

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

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

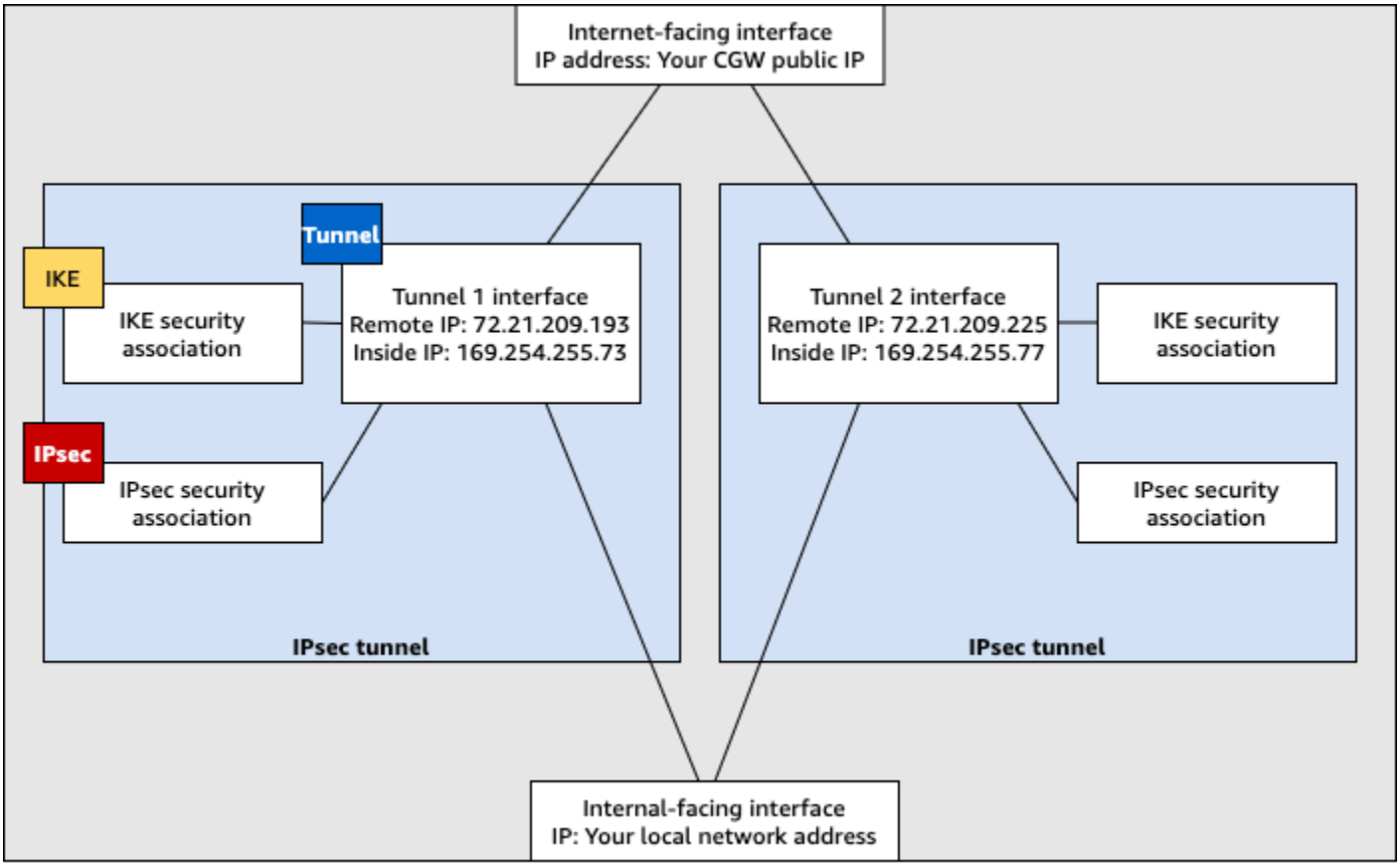
- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- Marcadores de posición para los puntos de enlace de direcciones IP remotas de AWS (externas) (*AWS_ENDPOINT_1* y *AWS_ENDPOINT_2*)

- Un marcador de posición de posición para la dirección IP de la interfaz externa direccionable a Internet en el dispositivo de gateway de cliente (*su-dirección-ip-cgw*).
- Un marcador de posición para el valor de clave previamente compartida (clave previamente compartida)
- 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 de cliente de AWS Site-to-Site VPN para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

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

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

Estos son los pasos para configurar su dispositivo de gateway de cliente si su dispositivo es un dispositivo Check Point Security Gateway que ejecuta R77.10 o una versión posterior utilizando el sistema operativo Gaia y Check Point SmartDashboard. También puede consultar el artículo Check Point Security Gateway IPsec VPN to Amazon Web Services VPC en el centro de soporte técnico de Check Point.

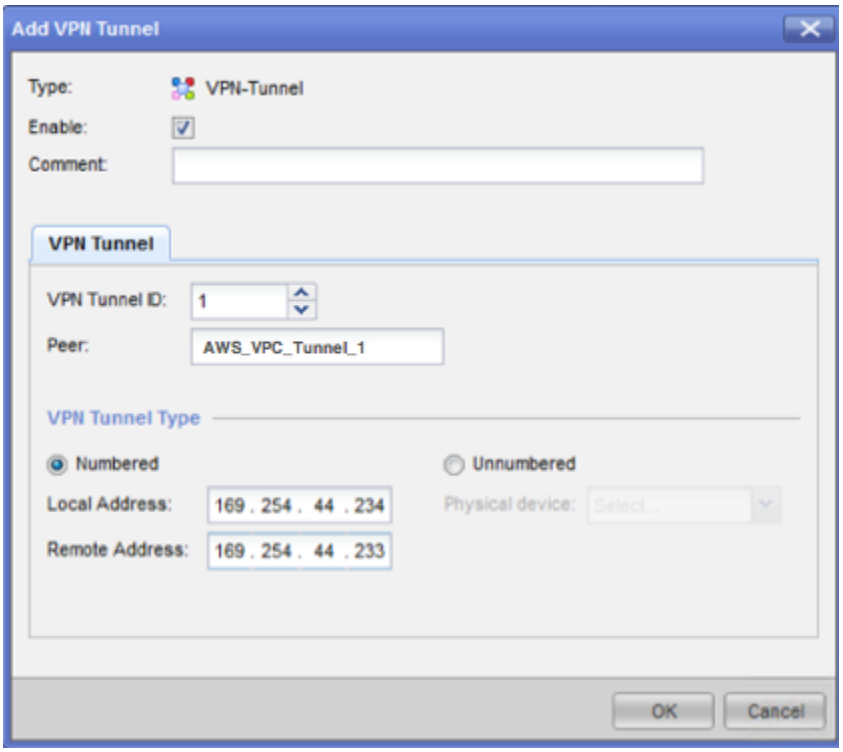
Para configurar la interfaz de túnel

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. 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:

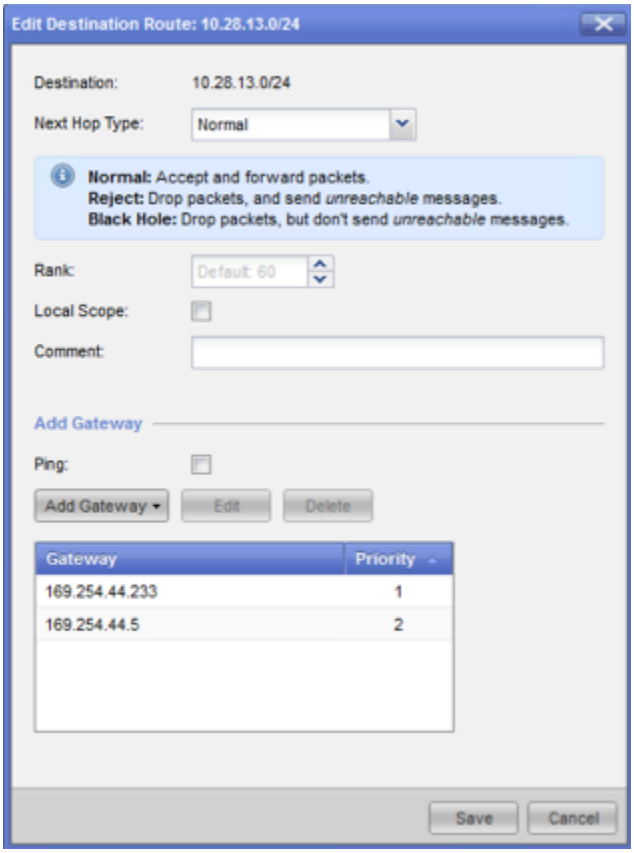
```
set interface vpnt2 mtu 1436
```

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 IPv4 Static Routes, Add.
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 Save.

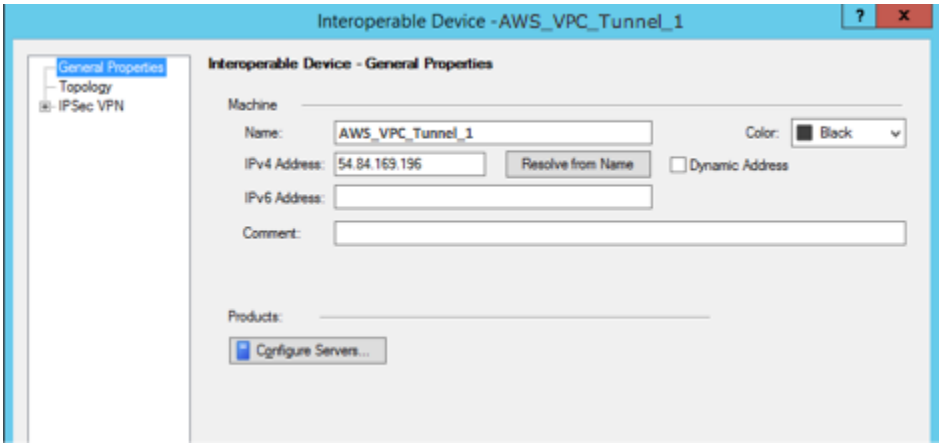
Si va a utilizar un clúster, repita los pasos anteriores para los demás miembros del clúster.

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. Abra Check Point 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. Para Name (Nombre), escriba el nombre que ha proporcionado para cada túnel, por ejemplo: `AWS_VPC_Tunnel_1` o `AWS_VPC_Tunnel_2`.

5. Para IPv4 Address, escriba la dirección IP externa de la gateway 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 su gateway y, en el panel Category, elija Topology.
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 Aceptar.

> **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.

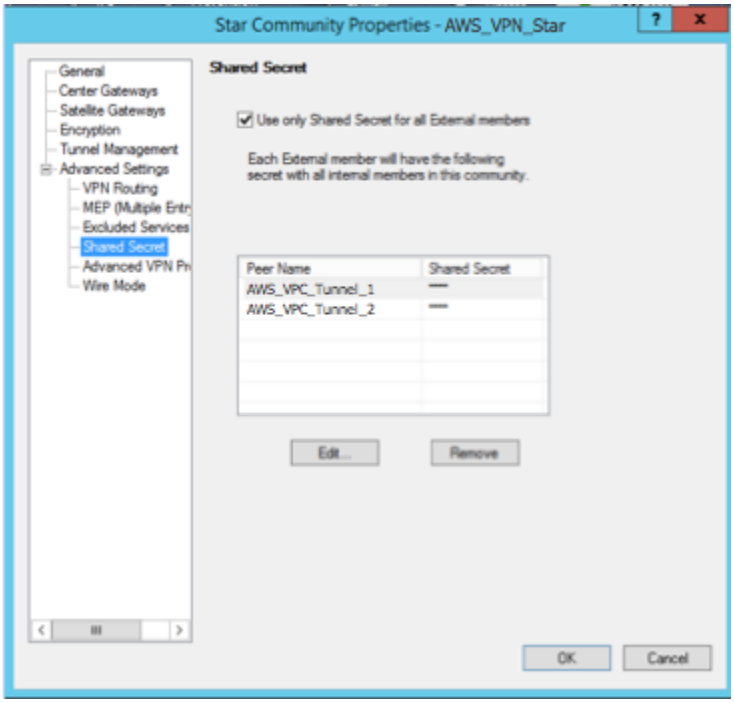
9. Repita estos pasos para crear un segundo objeto de red, utilizando la información de la sección `IPSec Tunnel #2` del archivo de configuración.

> **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 los ajustes de comunidad de VPN, IKE e 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 configurará los ajustes de intercambio de claves por Internet (IKE) y de IPsec.

1. En las propiedades de su gateway, elija IPSec VPN en el panel Category.
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 Encryption Method, elija IKEv1 only. 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
   - Propiedades de asociación de seguridad de IPsec (fase 2):
     - Perform IPsec data encryption with: 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`
        - Renegotiate IPsec security associations every `3600` seconds

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 SmartDashboard, elija Global Properties para su gateway. En el panel Category, expanda VPN y elija Advanced.
2. Elija Enable VPN Directional Match in VPN Column y guarde los cambios.

3. En 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 SmartDashboard, elija Policy, Install.
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 propiedad `tunnel_keepalive_method` utilizando la herramienta GuiDBedit.

1. Abra 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 ventanas de SmartConsole, como SmartDashboard, SmartView Tracker y SmartView Monitor.
4. Inicie la herramienta GuiBDedit. 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 herramienta GuiDBedit.
13. Abra 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.

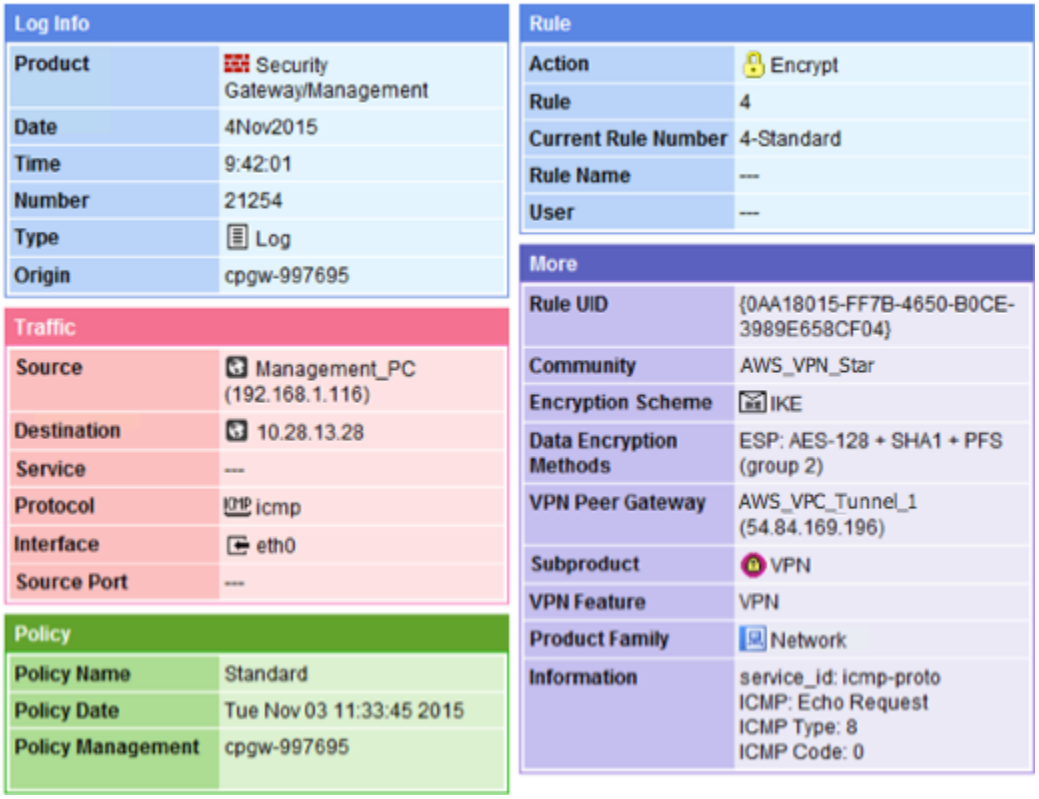
Para verificar el estado del túnel

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 verificar las asociaciones de IKE y 2 para verificar las asociaciones de IPsec.

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.
- Nombre o dirección de gateway principal de IPsec: escriba la dirección IP de la gateway privada virtual tal como se indica en el archivo de configuración (por ejemplo, `72.21.209.193`).
- IPsec Secondary Gateway Name or Address: 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.
- Local IKE ID: escriba la dirección IPv4 de la gateway de cliente (dispositivo SonicWALL).
- Peer IKE ID: escriba la dirección IPv4 de la gateway 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.
     - Authentication: elija SHA1 o SHA256.
     - Life Time: escriba `28800`.
   - En IKE (Phase 2) Proposal, haga lo siguiente:
     - Protocol: elija ESP.
     - Encryption: elija AES-128 o AES-256.
     - Authentication: elija SHA1 o SHA256.
     - Seleccione la casilla de verificación Enable Perfect Forward Secrecy y elija el grupo Diffie-Hellman.

- Life Time: escriba `3600`.

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

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 Aceptar. 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 ASA solo admiten el modo Active/Standby. Al utilizar estos Cisco ASA, solo puede tener un túnel activo cada 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.

Cisco ASA a partir de la versión 9.7.1 y posteriores admiten el modo Activo/Activo. Al utilizar estos Cisco ASA, 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.

- Asegurarse de que Crypto IPsec Transform Set y la secuencia de política de Crypto ISAKMP son coherentes con los demás túneles IPsec que están configurados 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 de cliente de AWS Site-to-Site VPN

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

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

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

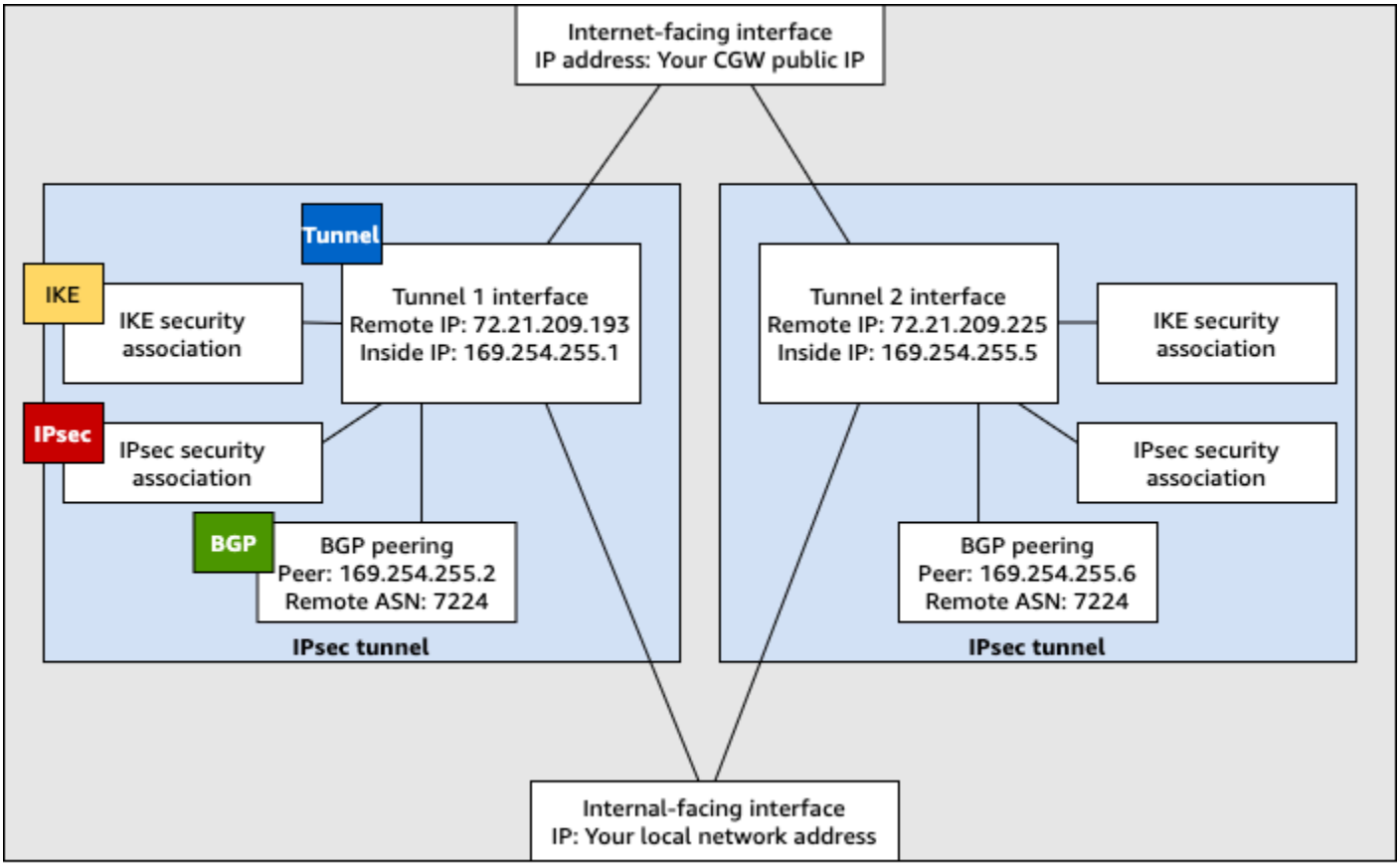
- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- Marcadores de posición para los puntos de enlace de direcciones IP remotas de AWS (externas) (*AWS_ENDPOINT_1* y *AWS_ENDPOINT_2*)
- Un marcador de posición de posición para la dirección IP de la interfaz externa direccionable a Internet en el dispositivo de gateway de cliente (*su-dirección-ip-cgw*).
- Un marcador de posición para el valor de clave previamente compartida (clave previamente compartida)
- 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 de

cliente de AWS Site-to-Site VPN para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

Además de proporcionar valores de marcadores de posición, en los archivos se especifican los requisitos mínimos para una conexión Site-to-Site VPN de AES128, SHA1 y grupo 2 de Diffie-Hellman en la mayoría de Regiones AWS, y AES128, SHA2 y Diffie-Hellman grupo 14 en las Regiones AWS de GovCloud. También se especifican claves previamente compartidas para la autenticación. Debe modificar el archivo de configuración de ejemplo para aprovecharse de los algoritmos de seguridad adicionales, los grupos 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 dinámico para un dispositivo de puerta de enlace de cliente de 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

Estos son los pasos para configurar un dispositivo Check Point Security Gateway con R77.10 o versiones posteriores utilizando 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 gateway de cliente (ASN que se proporcionó al crear la gateway de cliente en AWS) mediante la ejecución del comando siguiente.

   ```
   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 Save.

Para anunciar rutas locales

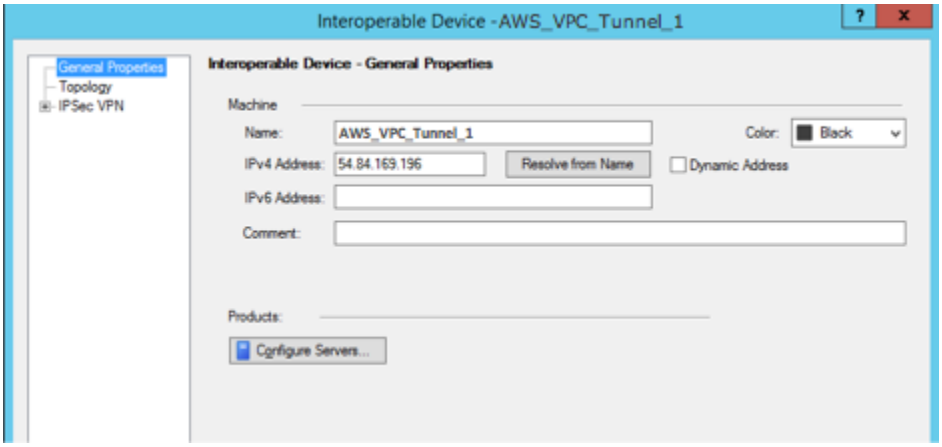
A continuación se presentan los pasos para distribuir rutas de interfaces locales. También puede redistribuir rutas desde distintos orígenes (por ejemplo, rutas estáticas o rutas obtenidas mediante protocolos de direccionamiento dinámico). Para obtener más información, consulte la Gaia Advanced Routing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

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 Check Point 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. Para IPv4 Address, escriba la dirección IP externa de la gateway 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 Aceptar.
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 Aceptar.

> **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 los ajustes de comunidad de VPN, IKE e IPsec

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 configurará los ajustes de intercambio de claves por Internet (IKE) y de IPsec.

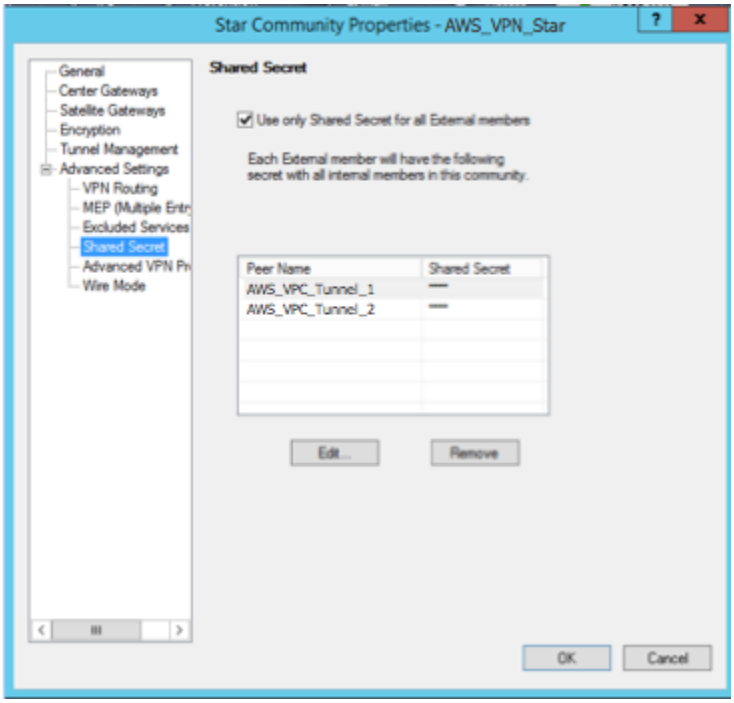
1. En las propiedades de su gateway, elija IPSec VPN en el panel Category.
2. Elija Communities, New, Star Community.
3. Proporcione un nombre para su comunidad (por ejemplo, `AWS_VPN_Star`) y, a continuación, elija Center Gateways en el panel Category.
4. Elija Add y agregue su gateway o clúster a la 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 Encryption Method, elija IKEv1 for IPv4 and IKEv2 for IPv6. En la sección Encryption Suite, elija Custom, Custom Encryption.

   > **Note**
   >
   > Debe seleccionar la opción IKEv1 para IPv4 e IKEv2 para IPv6 para la funcionalidad IKEv1.

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
   - Propiedades de asociación de seguridad de IPsec (fase 2):
     - Perform IPsec data encryption with: 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)`
        - Renegotiate IPsec security associations every `3600` seconds

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 SmartDashboard, elija Global Properties para su gateway. En el panel Category, expanda VPN y elija Advanced.
2. Elija Enable VPN Directional Match in VPN Column y elija OK.
3. En 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 SmartDashboard, elija Policy, Install.
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 propiedad `tunnel_keepalive_method` utilizando la herramienta GuiDBedit.

1. Abra 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 ventanas de SmartConsole, como SmartDashboard, SmartView Tracker y SmartView Monitor.
4. Inicie la herramienta GuiBDedit. 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 herramienta GuiDBedit.
13. Abra 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).

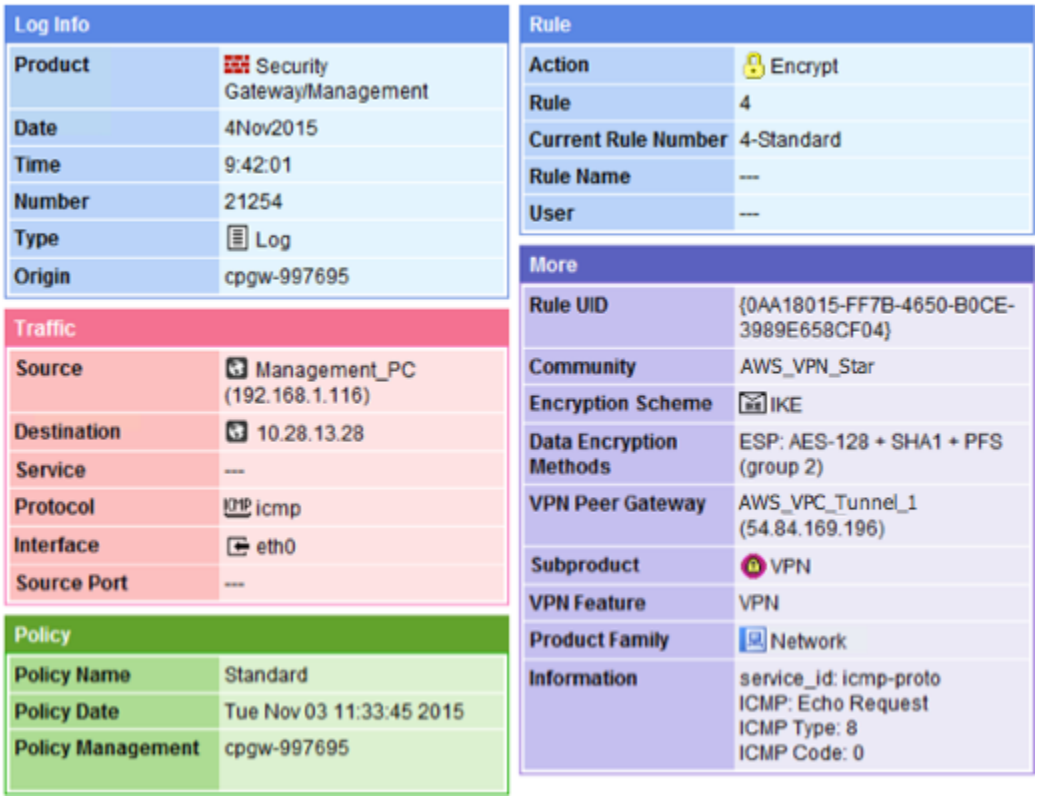
Para verificar el estado del túnel

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 verificar las asociaciones de IKE y 2 para verificar las asociaciones de IPsec.

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 ASA solo admiten el modo Active/Standby. Al utilizar estos Cisco ASA, solo puede tener un túnel activo cada 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.

Cisco ASA a partir de la versión 9.7.1 y posteriores admiten el modo Activo/Activo. Al utilizar estos Cisco ASA, 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.
- Asegurarse de que Crypto IPsec Transform Set y la secuencia de política de Crypto ISAKMP son coherentes con los demás túneles IPsec que están configurados 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 externa se conoce como *ge-0/0/0.0*.
- Los ID de la interfaz de túnel se conocen como *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").

Configuración de Windows Server como dispositivo de puerta de enlace de cliente de AWS Site-to-Site VPN

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 instancia de EC2 en una VPC o en su propio servidor. Los siguientes procedimientos se aplican a Windows Server 2012 R2 y versiones posteriores.

Contenido

Configuración de instancias de Windows

Si configura Windows Server en una instancia EC2 iniciada desde una AMI de Windows, haga lo siguiente:

- Deshabilite la comprobación de origen/destino para la instancia:
  1. Abra la consola de Amazon EC2 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 Advanced, deshabilite las propiedades IPv4 Checksum Offload, TCP Checksum Offload (IPv4) y UDP Checksum Offload (IPv4) y, a continuación, elija OK.
- 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 usuario de Amazon EC2. Anote esta dirección, ya que la necesitará para crear la puerta de enlace de cliente.
- Asegúrese de que las reglas del grupo de seguridad de su instancia permiten el tráfico IPsec saliente. De forma predeterminada, un grupo de seguridad permite todo el tráfico saliente. No obstante, si el estado original de las reglas salientes del grupo de seguridad se ha modificado, debe crear las siguientes reglas de protocolo personalizadas de salida para el tráfico IPsec: 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.

Para 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 (Conexiones de Site-to-Site VPN).
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 de VPN en el extremo de AWS 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`

Clave previamente compartida que se utiliza para establecer la conexión de VPN IPsec entre el `Local Tunnel Endpoint` y el `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 de un dispositivo en AWS, su conexión de VPN cambiará 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**
>
> En ocasiones, AWS realiza tareas de mantenimiento de rutina 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.

La información adicional acerca del intercambio de claves por Internet (IKE) y las asociaciones de seguridad de IPsec (SA) se muestran en el archivo de configuración descargado.

```
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 destinadas a la conexión VPN y la configuración predeterminada para las conexiones VPN IPsec del servidor de Windows.

`MainModeKeyLifetime`

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

`QuickModeSecMethods`

Algoritmos de cifrado y autenticación para IPsec SA. Estas son las configuraciones sugeridas destinadas a la conexión VPN y la configuración predeterminada para las conexiones VPN IPsec del servidor de Windows.

`QuickModePFS`

Se recomienda utilizar la confidencialidad directa total (PFS) de clave maestra para las sesiones de IPsec.

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, seleccione Acceso directo y 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**
>
> Se recomienda que utilice la confidencialidad directa total (PFS) de clave maestra para las sesiones de IPsec. Si elige ejecutar el script netsh, comprobará que 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: escriba la dirección IP privada del servidor de Windows en 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 de netsh, consulte Netsh AdvFirewall Consec Commands 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

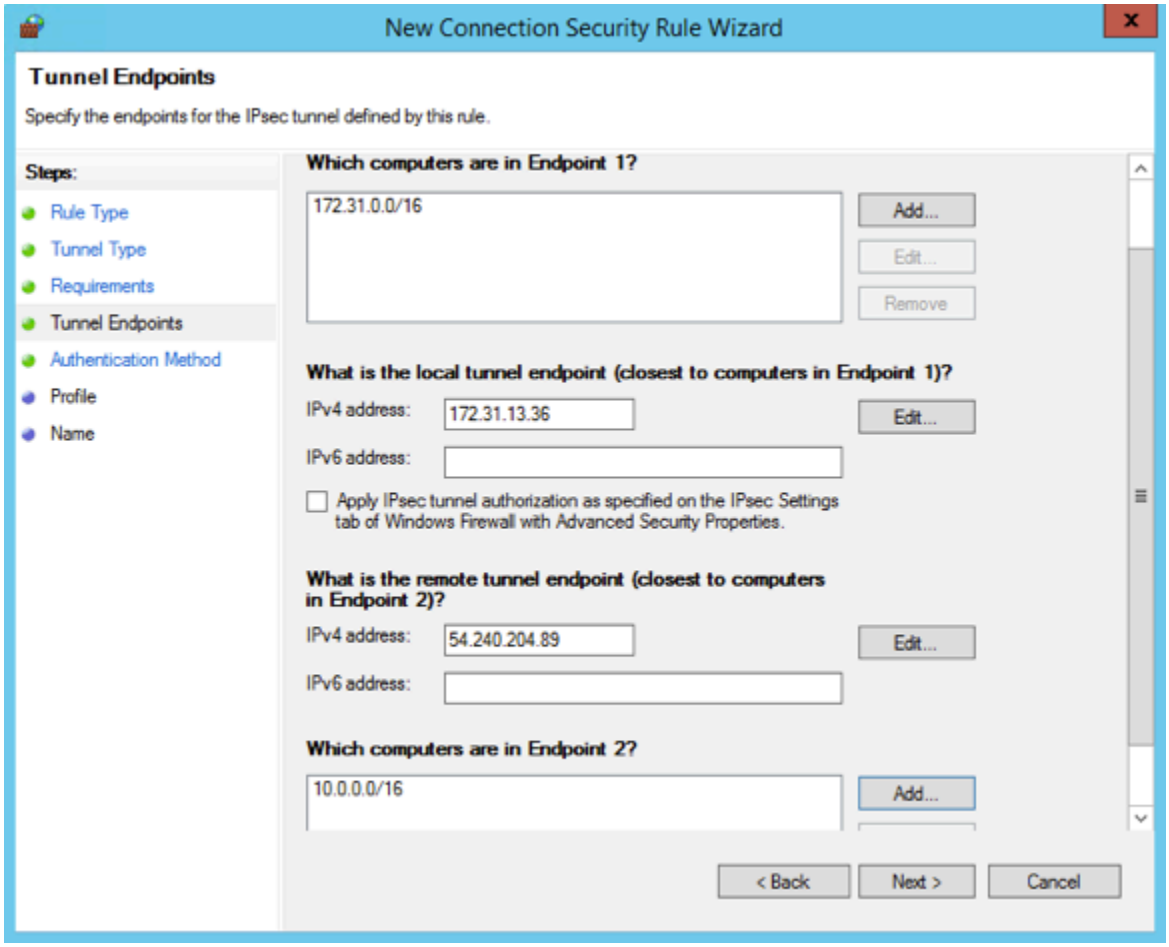
1. Abra el administrador del servidor, elija Tools (Herramientas)y, a continuación, seleccione Windows Defender Firewall with Advanced Security (Firewall de Windows Defender con seguridad avanzada).
2. Seleccione Reglas de seguridad de conexión, elija Acción y, a continuación, Nueva regla.
3. En el Asistente 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 las conexiones protegidas por IPsec de este túnel?, deje el valor predeterminado activado (No. Enviar todo el tráfico de red que coincida con esta regla de seguridad de la conexión por el túnel.) y, a continuación, elija 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 IPv4 address (Dirección IPv4), escriba la dirección IP privada del servidor de Windows y, a continuación, elija OK (Aceptar).
8. En ¿Cuál es el extremo de túnel remoto (más cercano a los equipos del Extremo 2)?, elija Editar. En el campo Dirección IPv4, escriba la dirección IP de la gateway privada virtual del Túnel 1 del archivo de configuración (consulte `Remote Tunnel Endpoint`) y, a continuación, elija 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 Siguiente.

16. En la página Perfil, active las tres casillas de verificación: Dominio, Privado y Público. Elija 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 Túnel IPsec, elija Personalizar. Compruebe los siguientes parámetros de túnel IPsec y, a continuación, elija Aceptar. A continuación, vuelva a seleccionar Aceptar para cerrar el cuadro de diálogo.

   - La opción Usar túnel IPsec está seleccionada.
   - El punto de enlace del túnel local (más cercano al punto de enlace 1) contiene la dirección IP del servidor de Windows. Si su dispositivo de gateway de cliente es una instancia EC2, deberá indicar 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 sus reglas de seguridad en el servidor, configure algunos ajustes básicos de IPsec para trabajar con la gateway 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 Configuración IPsec, en Exenciones IPsec, asegúrese de que la opción ICMP está exento de IPsec está configurada con el valor No (predeterminado). Asegúrese de que la opción Autorización de túnel IPsec está configurada con la opción Ninguno.
3. En Predeterminados de IPsec, 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. Elija Aceptar para volver al cuadro de diálogo Personalizar configuración IPsec y elija 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 el servidor de Windows, inicie el símbolo del sistema o una sesión de PowerShell y escriba regedit para iniciar el editor del registro.
2. Expanda HKEY_LOCAL_MACHINE, SYSTEM, CurrentControlSet, Services, Tcpip y, a continuación, Parameters.
3. Desde el menú Editar, seleccione Nuevo y seleccione Valor de DWORD (32 bits).
4. Escriba el nombre EnableDeadGWDetect.
5. Seleccione EnableDeadGWDetect y elija Edit (Editar), Modify (Modificar).
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 EnableDeadGWDetect en la Biblioteca de Microsoft TechNet.

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 Prueba de una conexión de AWS Site-to-Site VPN.

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 el servidor de Windows es una instancia EC2, asegúrese de que las reglas salientes de su grupo de seguridad permiten el tráfico IPsec. 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 una de las AMI de Amazon Linux.
- Si la instancia a la que va a hacer ping es una instancia de Windows, conéctese a la instancia y habilite ICMPv4 entrante 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 gateway del cliente es una instancia EC2, asegúrese de que ha deshabilitado la comprobación de origen o 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 del dispositivo de puerta de enlace de cliente de AWS Site-to-Site VPN

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 VPNRegistros de puede ser útil para solucionar problemas de conectividad de VPN. Para instrucciones de prueba generales, consulte también Prueba de una conexión de AWS Site-to-Site VPN.

Temas

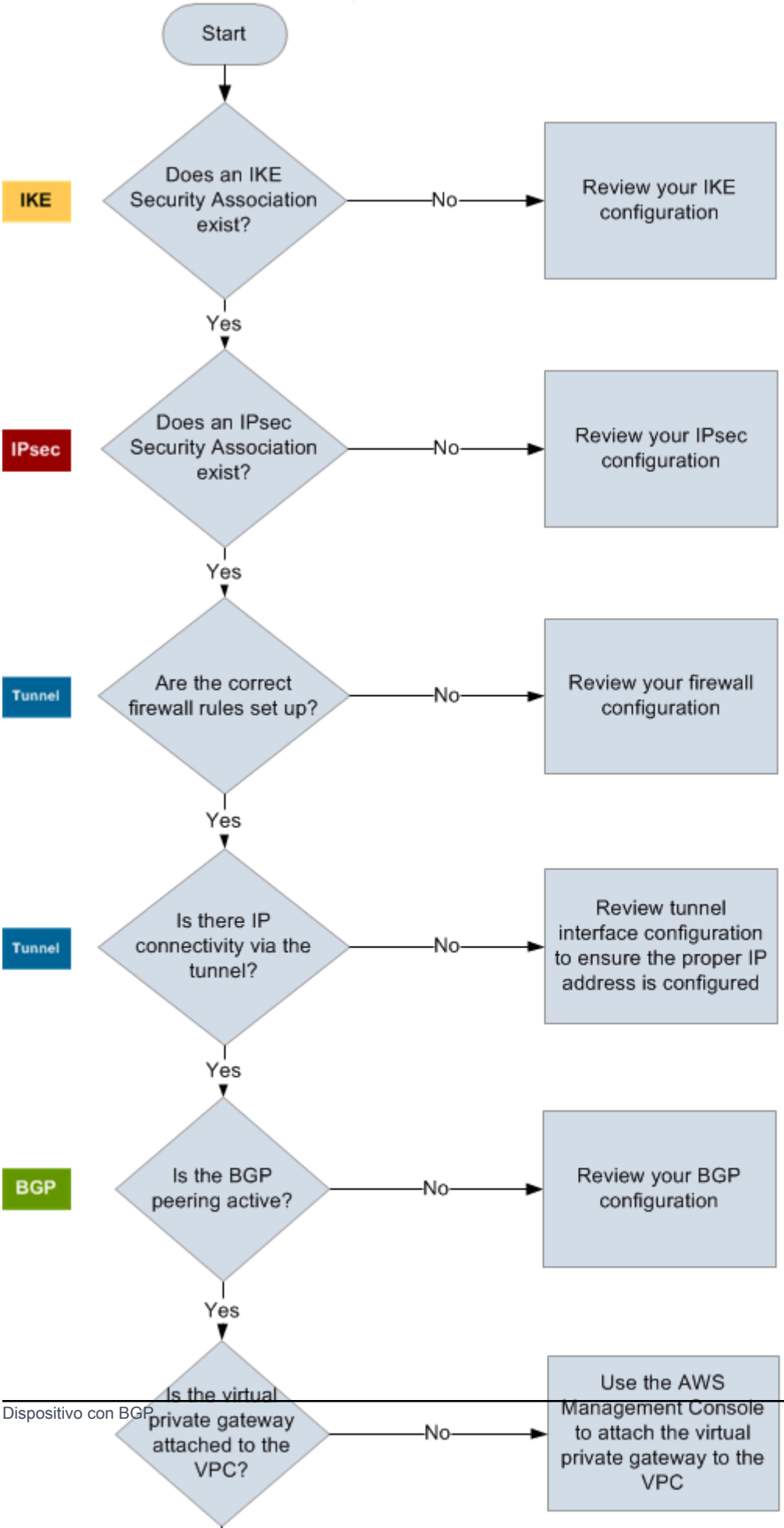
- Solución de problemas de conectividad de AWS Site-to-Site VPN al usar el protocolo de puerta de enlace fronteriza
- Solución de problemas de conectividad de AWS Site-to-Site VPN sin protocolo de puerta de enlace fronteriza
- Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Cisco ASA
- Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Cisco IOS
- Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Cisco IOS sin protocolo de puerta de enlace fronteriza
- Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Juniper JunOS
- Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Juniper ScreenOS
- Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Yamaha

Recursos adicionales

- Foro de Amazon VPC

Solución de problemas de conectividad de AWS Site-to-Site VPN al usar el protocolo de puerta de enlace fronteriza

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.

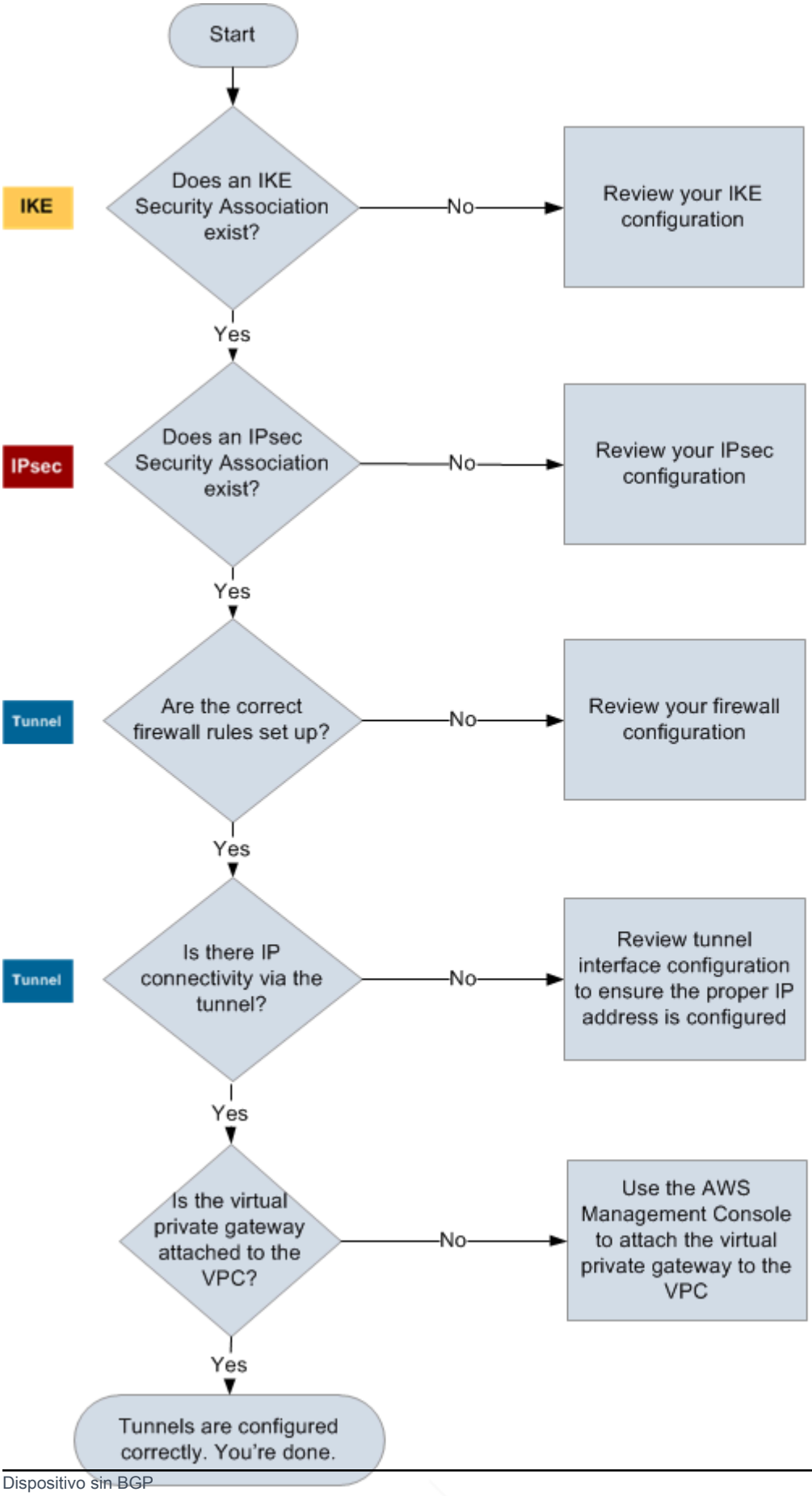

Start
IKE
Does an IKE Security Association exist?
No
Review your IKE configuration
Yes
IPsec
Does an IPsec Security Association exist?
No
Review your IPsec configuration
Yes
Tunnel
Are the correct firewall rules set up?
No
Review your firewall configuration
Yes
Tunnel
Is there IP connectivity via the 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. Es necesario tener una asociación de seguridad de IKE para intercambiar las claves que se utilizan para establecer la asociación de seguridad de IPsec. 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 de IKE, continúe hasta “IPsec”.
IPsec	Determine si existe una asociación de seguridad (SA) de IPsec. Una SA de IPSec es el propio túnel. Consulte el dispositivo de gateway de cliente para determinar si hay activa una SA de IPSec. Asegúrese de configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo mostrado en el archivo de configuración. Si no existe una SA de IPSec, revise la configuración de IPSec. Si existe una SA de IPSec, vaya a la sección “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 de cliente de AWS Site-to-Site VPN). 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.

Solución de problemas de conectividad de AWS Site-to-Site VPN sin protocolo de puerta de enlace fronteriza

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. Es necesario tener una asociación de seguridad de IKE para intercambiar las claves que se utilizan para establecer la asociación de seguridad de IPsec. 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 de IKE, continúe hasta “IPsec”.
IPsec	Determine si existe una asociación de seguridad (SA) de IPsec. Una SA de IPSec es el propio túnel. Consulte el dispositivo de gateway de cliente para determinar si hay activa una SA de IPSec. Asegúrese de configurar los parámetros de cifrado, autenticación, confidencialidad directa total y modo según lo mostrado en el archivo de configuración. Si no existe una SA de IPSec, revise la configuración de IPSec. Si existe una SA de IPSec, vaya a la sección “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 de cliente de AWS Site-to-Site VPN). 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.

Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Cisco ASA

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Cisco, tenga en cuenta el IKE, el IPsec y el direccionamiento. 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 Cisco ASA solo admiten el modo Active/Standby. Al utilizar estos Cisco ASA, solo puede tener un túnel activo cada 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 mostrará un dispositivo de gateway de cliente con 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 integ-ppe-loopback extended permit ip any vpc_subnet subnet_mask
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (vpc_subnet/subnet_mask/0/0)
      current_peer: integ-ppe1
```

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

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

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

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

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

En Cisco ASA, IPsec solo aparece después de enviar tráfico interesante (tráfico que debe cifrarse). Para mantener IPsec siempre activo, recomendamos configurar una monitorización de SLA. La monitorización de SLA sigue enviando tráfico interesante, lo que mantendrá el IPsec activo.

También puede utilizar el siguiente comando ping para obligar a su IPsec a comenzar la negociación y continuar.

```
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 funciona, se debe establecer el IPSec. En caso contrario, compruebe sus listas de acceso y consulte la sección anterior de IPsec.

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 comando traceroute desde el dispositivo Cisco ASA para ver si llega a los routers de 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.

Rebote de la interfaz del túnel

Si el túnel parece estar activo pero el tráfico no fluye correctamente, el rebote de la interfaz del túnel (deshabilitándola y volviendo a habilitarla) suele resolver problemas de conectividad. Cómo 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
```

También puede utilizar un comando de una sola línea:

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

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

Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Cisco IOS

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Cisco, tenga en cuenta cuatro elementos: IKE, IPsec, el 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.

```
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 mostrará un dispositivo de gateway de cliente con 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`. Si aparece una SA (`spi: 0xF95D2F3C`, por ejemplo) y el valor de `Status` es `ACTIVE`, IPsec se ha configurado correctamente.

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 de cliente de AWS Site-to-Site VPN.

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.

Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Cisco IOS sin protocolo de puerta de enlace fronteriza

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Cisco, tenga en cuenta tres elementos: IKE, IPsec y el 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 mostrará un dispositivo de gateway de cliente con 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 indica que aparece una SA (por ejemplo, `spi: 0x48B456A6`), que el estado es `ACTIVE` y que IPsec se ha configurado 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 de cliente de AWS Site-to-Site VPN.

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.

Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Juniper JunOS

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Juniper, tenga en cuenta cuatro elementos: IKE, IPsec, el 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 mostrará un dispositivo de gateway de cliente con IPsec configurado correctamente.

```
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 de cliente de AWS Site-to-Site VPN.

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
```

Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Juniper ScreenOS

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente basado en Juniper ScreenOS, tenga en cuenta cuatro elementos: IKE, IPsec, el 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 e 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 de cliente de AWS Site-to-Site VPN.

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
```

Solución de problemas de conectividad de AWS Site-to-Site VPN con un dispositivo de puerta de enlace de cliente de Yamaha

Al solucionar problemas de conectividad de un dispositivo de gateway de cliente de Yamaha, tenga en cuenta cuatro elementos: IKE, IPsec, el 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 para conectarse a Site-to-Site VPN. Si el `proxy ID` no está configurado en el enrutador, consulte el archivo de configuración de ejemplo que proporciona AWS para que Yamaha se 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 (SA) 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 mostrará un dispositivo de gateway de cliente con 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 de cliente de AWS Site-to-Site VPN.

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 valor `current status` esté online y que `Interface type` sea 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
```

Trabajar con de AWS Site-to-Site VPN

Puede utilizar los recursos de Site-to-Site VPN a través de la consola de Amazon VPC o la AWS CLI.

Temas

Creación de un archivo adjunto de AWS Site-to-Site VPN para WAN en la nube de AWS

Puede crear una conexión de Site-to-Site VPN para WAN en la nube de AWS mediante el siguiente procedimiento. Para obtener más información sobre los archivos adjuntos de la VPN y WAN en la nube, consulte archivos adjuntos de Site-to-Site VPN en WAN en la nube de AWS en la Guía del usuario de WAN en la nube de AWS.

Las conexiones de la VPN de WAN en la nube son compatibles con los protocolos IPv4 e IPv6. Para obtener más información sobre el uso de cualquiera de estos protocolos para una conexión de VPN de WAN en la nube, consulte Tráfico de IPv4 e IPv6 en AWS Site-to-Site VPN.

Para crear una asociación 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, elija Conexiones de 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 utilizar una puerta de enlace de cliente existente, elija Existente y, a continuación, elija ID de puerta de enlace de cliente.
   - Para crear una nueva puerta de enlace de cliente, elija Nueva.
     1. En Dirección IP, introduzca una dirección IPv4 o IPv6 de destino.
     2. En ARN de certificado, elija el ARN de su certificado privado (si utiliza 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. En Opciones de enrutamiento, elija Dinámico (requiere BGP) o Estático.
8. En Almacenamiento de claves compartidas previamente, elija Estándar o Secrets Manager. La selección predeterminada es Estándar. Para obtener más información acerca del uso de AWS Secrets Manager, consulte Seguridad.
9. En Túnel dentro de la versión de IP, elija IPv4 o IPv6.
10. (Opcional) En Habilitar 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.
11. (Opcional) Según qué túnel de la versión de IP haya elegido, realice una de las siguientes operaciones:
    - IPv4: en CIDR de red IPv4 local, especifique el intervalo de CIDR de IPv4 en el extremo de la puerta de enlace de cliente (en las instalaciones) que puede comunicarse a través de los túneles de VPN. En CIDR de red IPv4 remoto, especifique el intervalo de CIDR en el extremo de AWS que se puede comunicar a través de los túneles de VPN. El valor predeterminado de ambos campos es `0.0.0.0/0`.

- IPv6: en CIDR de red IPv6 local, especifique el intervalo de CIDR de IPv6 en el extremo de la puerta de enlace de cliente (en las instalaciones) que puede comunicarse a través de los túneles de VPN. En CIDR de red IPv6 remoto, especifique el intervalo de CIDR en el extremo de AWS que se puede comunicar a través de los túneles de VPN. El valor predeterminado de ambos campos es `::/0`

12. En Tipo de dirección IP externa, elija una de las siguientes opciones:

- IPv4 público: (predeterminado) utilice direcciones IPv4 para las IP de túnel externo.
- IPv4 privada: utilice una dirección IPv4 privada para utilizarla en redes privadas.
- IPv6: utilice direcciones IPv6 para las IP de túnel externo. Esta opción requiere que el dispositivo de puerta de enlace de cliente admita direcciones IPv6.

> **Note**
>
> Si selecciona IPv6 como tipo de dirección IP externa, debe crear una puerta de enlace de cliente con una dirección IPv6

13. (Opcional) En Opciones de túnel 1, puede especificar la siguiente información para cada túnel:

- Un bloque CIDR IPv4 de tamaño /30 desde el rango `169.254.0.0/16` para las direcciones IPv4 de túnel interior.
- Si especificó IPv6 en Túnel dentro de la versión IP, un bloque de CIDR IPv6 /126 del intervalo `fd00::/8` para las direcciones IPv6 del túnel interior.
- La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: 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 Habilitar para Registro de actividad del túnel para capturar mensajes de registro de la actividad de IPSec y los mensajes del protocolo DPD.
- (Opcional) Seleccione Activar para Ciclo de vida de puntos de conexión de túnel para controlar la programación de sustituciones de puntos de conexión. Para obtener más información sobre el ciclo de vida de un punto de conexión, consulte Ciclo de vida del punto de conexión del túnel.

14. (Opcional) Elija Opciones de túnel 2 y siga los pasos anteriores para configurar un segundo túnel.

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

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

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

  Ejemplo de creación de una conexión de VPN con IP de túnel externo IPv6 e IP de túnel interno IPv6:

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

Creación de una conexión de puerta de enlace de tránsito de AWS Site-to-Site VPN

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.

Las conexiones de VPN de puerta de enlace de tránsito son compatibles con IPv4 e IPv6. Para obtener más información sobre el uso de cualquiera de estos protocolos para una conexión de VPN de puerta de enlace de tránsito, consulte Tráfico de IPv4 e IPv6 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 de 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 utilizar una puerta de enlace de cliente existente, elija Existente y, a continuación, elija ID de puerta de enlace de cliente.
   - Para crear una nueva puerta de enlace de cliente, elija Nueva.
     1. En Dirección IP, introduzca una dirección IPv4 o IPv6 de destino.
     2. En ARN de certificado, elija el ARN de su certificado privado (si utiliza 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. En Opciones de enrutamiento, elija Dinámico (requiere BGP) o Estático.
8. En Almacenamiento de claves compartidas previamente, elija Estándar o Secrets Manager. La selección predeterminada es Estándar. Para obtener más información acerca del uso de AWS Secrets Manager, consulte Seguridad.
9. En Túnel dentro de la versión de IP, elija IPv4 o IPv6.
10. (Opcional) En Habilitar 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.
11. (Opcional) Según qué túnel de la versión de IP haya elegido, realice una de las siguientes operaciones:
    - IPv4: en CIDR de red IPv4 local, especifique el intervalo de CIDR de IPv4 en el extremo de la puerta de enlace de cliente (en las instalaciones) que puede comunicarse a través de los túneles de VPN. En CIDR de red IPv4 remoto, especifique el intervalo de CIDR en el extremo de AWS que se puede comunicar a través de los túneles de VPN. El valor predeterminado de ambos campos es `0.0.0.0/0`.
    - IPv6: en CIDR de red IPv6 local, especifique el intervalo de CIDR de IPv6 en el extremo de la puerta de enlace de cliente (en las instalaciones) que puede comunicarse a través de los túneles de VPN. En CIDR de red IPv6 remoto, especifique el intervalo de CIDR en el extremo de AWS que se puede comunicar a través de los túneles de VPN. El valor predeterminado de ambos campos es `::/0`

12. En Tipo de dirección IP externa, elija una de las siguientes opciones:

    - IPv4 público: (predeterminado) utilice direcciones IPv4 para las IP de túnel externo.
    - IPv4 privada: utilice una dirección IPv4 privada para utilizarla en redes privadas.
    - IPv6: utilice direcciones IPv6 para las IP de túnel externo. Esta opción requiere que el dispositivo de puerta de enlace de cliente admita direcciones IPv6.

    > **Note**
    >
    > Si selecciona IPv6 como tipo de dirección IP externa, debe crear una puerta de enlace de cliente con una dirección IPv6

13. (Opcional) En Opciones de túnel 1, puede especificar la siguiente información para cada túnel:

    - Un bloque CIDR IPv4 de tamaño /30 desde el rango `169.254.0.0/16` para las direcciones IPv4 de túnel interior.
    - Si especificó IPv6 en Túnel dentro de la versión IP, un bloque de CIDR IPv6 /126 del intervalo `fd00::/8` para las direcciones IPv6 del túnel interior.
    - La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: 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 Habilitar para Registro de actividad del túnel para capturar mensajes de registro de la actividad de IPSec y los mensajes del protocolo DPD.
    - (Opcional) Seleccione Activar para Ciclo de vida de puntos de conexión de túnel para controlar la programación de sustituciones de puntos de conexión. Para obtener más información sobre el ciclo de vida de un punto de conexión, consulte Ciclo de vida del punto de conexión del túnel.

14. (Opcional) Elija Opciones de túnel 2 y siga los pasos anteriores para configurar un segundo túnel.
15. Elija Create VPN Connection (Crear conexión VPN).

Creación de una conexión de VPN con la CLI

Utilice el comando create-vpn-connection y especifique el ID de la gateway de tránsito en la opción `--transit-gateway-id`.

Ejemplo de creación de una conexión de VPN con IP de túnel externo IPv6 e IP de túnel interno IPv6:

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

Ejemplo de creación de una conexión de VPN con IP de túnel externo IPv6 e IP de túnel interno IPv4:

```
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 de las direcciones IPv6 para la conexión de VPN

Tras crear una conexión de VPN con IP de túnel externo IPv6, puede ver las direcciones IPv6 asignadas mediante el comando `describe-vpn-connections` de la CLI:

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

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

Extracto de respuesta de ejemplo:

```
"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",
            ...
        }
    ]
}
```

Prueba de una conexión de AWS Site-to-Site VPN

Después de crear la conexión de AWS Site-to-Site VPN y de configurar la gateway de 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 una de las AMI de Amazon Linux.
- 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 va a utilizar instancias que ejecuten Windows Server, conecte la instancia y habilite el tráfico ICMPv4 entrante en el firewall de Windows para poder 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. Abra la consola de Amazon EC2 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). En la consola de Amazon EC2, se muestra la dirección en los datos 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 de AWS a la red en las instalaciones, puede utilizar SSH o RDP para conectarse 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 acerca de cómo conectarse a una instancia de Linux, consulte Conexión a la instancia de Linux en la Guía del usuario de Amazon EC2. Para obtener más información acerca de cómo conectarse a una instancia de Windows, consulte Conexión a la instancia de Windows en la Guía del usuario de Amazon EC2.

Eliminación de una conexión de AWS Site-to-Site VPN y una puerta de enlace

Si ya no necesita la conexión de AWS Site-to-Site VPN, puede eliminarla. Cuando elimina una conexión de Site-to-Site VPN, no se elimina la gateway de cliente ni la gateway privada virtual asociada a la conexión. Si ya no necesita la gateway de cliente ni la gateway privada virtual, puede eliminarlas.

> **Warning**
>
> Si elimina su conexión de Site-to-Site VPN y luego crea una nueva, deberá descargar un nuevo archivo de configuración y volver a configurar el dispositivo de puerta de enlace de cliente.

Tareas

- Eliminación de una conexión de AWS Site-to-Site VPN
- Eliminación de una puerta de enlace de cliente de AWS Site-to-Site VPN
- Desasociación y eliminación de una puerta de enlace privada virtual en AWS Site-to-Site VPN

Eliminación de una conexión de AWS Site-to-Site VPN

Cuando se elimina una conexión de Site-to-Site VPN, esta permanece visible durante un breve espacio de tiempo con el estado `deleted` y después se borra 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, elija Conexiones de 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 consulta de Amazon EC2)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (AWS Tools for Windows PowerShell)

Eliminación de una puerta de enlace de cliente de AWS Site-to-Site VPN

Si ya no necesita una gateway de cliente, puede eliminarla. No se pueden eliminar las gateways de cliente que se están utilizando en una conexión de 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 consulta de Amazon EC2)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (AWS Tools for Windows PowerShell)

Desasociación y eliminación de 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 consulta de Amazon EC2)
- 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 consulta de Amazon EC2)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (AWS Tools for Windows PowerShell)

Modificación de la puerta de enlace de destino de una conexión de AWS Site-to-Site VPN

Puede modificar la puerta de enlace de destino de una conexión de AWS Site-to-Site VPN. 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 gateway de destino, la conexión de Site-to-Site VPN no estará disponible durante un breve período de tiempo, mientras se aprovisionan los nuevos puntos de enlace.

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 gateway de destino es una gateway de tránsito, asocie las VPC a la gateway 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. Seleccione Save changes (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, elija Conexiones de 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. Seleccione Save changes (Guardar cambios).

Para modificar una conexión de Site-to-Site VPN a través de la línea de comandos o la API

- ModifyVpnConnection (API de consulta de Amazon EC2)
- 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

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
		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.
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)

Si la nueva gateway es de tránsito, modifique la tabla de enrutamiento de la gateway de tránsito para que permita el tráfico entre la VPC y 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 gateway de cliente para su conexión de AWS Site-to-Site VPN.

Modificación de las opciones de conexión de AWS Site-to-Site VPN

Puede modificar las opciones de una conexión de Site-to-Site VPN. Puede modificar las siguientes opciones:

- Los rangos de CIDR IPv4 en el lado local (gateway de cliente) y en el lado remoto (AWS) de la conexión de VPN que puede comunicarse a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0` para ambos rangos.
- Los rangos de CIDR IPv6 en el lado local (gateway de cliente) y remoto (AWS) de la conexión de VPN que puede comunicarse a través de los túneles de VPN. El valor predeterminado es `::/0` para ambos rangos.

Al modificar las opciones de conexión de VPN, las direcciones IP del punto de conexión de la VPN en el extremo de AWS no cambian y las opciones de 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, elija Conexiones de 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. Seleccione Save changes (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 consulta de Amazon EC2)

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

Puede modificar las opciones de los túneles de VPN de la conexión de 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, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de Site-to-Site VPN y elija Acciones, Modificar las opciones de túnel de 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. Seleccione Save changes (Guardar cambios).

Para modificar las opciones del túnel de VPN utilizando la línea de comandos o la API

- (AWS CLI) Utilice describe-vpn-connections para ver las opciones de túnel actuales y modify-vpn-tunnel-options para modificar las opciones de túnel.
- (API de consulta de Amazon EC2) Utilice DescribeVpnConnections para consultar las opciones actuales del túnel y ModifyVpnTunnelOptions para modificarlas.

Edición de rutas estáticas para una conexión de AWS Site-to-Site VPN

En las conexiones de Site-to-Site VPN de una puerta de enlace privada virtual configurada para un enrutamiento estático, puede agregar o eliminar rutas estáticas en la configuración de 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, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de VPN.
4. Elija Editar rutas estáticas.
5. Agregue o elimine rutas según sea necesario.
6. Seleccione Save changes (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 consulta de Amazon EC2)
- 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 consulta de Amazon EC2)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (AWS Tools for Windows PowerShell)

Cambio de la puerta de enlace de cliente para una conexión de AWS Site-to-Site VPN

Puede cambiar la gateway de cliente de una conexión Site-to-Site VPN utilizando 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, elija Conexiones de 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. Seleccione Save changes (Guardar cambios).

Para modificar la gateway de cliente mediante la línea de comando o API

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

Sustitución de las credenciales comprometidas por una conexión de AWS Site-to-Site VPN

Si cree que las credenciales del túnel de la conexión de Site-to-Site VPN se han visto comprometidas, puede cambiar la clave de IKE previamente compartida o el certificado de 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 VPNOpciones de autenticación de túneles de .

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

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. Puede especificar sus propias claves compartidas previamente para los túneles o permitir a AWS generar nuevas claves compartidas previamente para usted. 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 de AWS del punto de enlace 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.

Rotación de certificados de punto de conexión de túnel de AWS Site-to-Site VPN

Puede rotar los certificados de los puntos de conexión del túnel en el extremo de AWS a través de la consola de Amazon VPC. Cuando el certificado de un punto de enlace de túnel esté a punto de caducar, AWS rota automáticamente el certificado utilizando el rol vinculado al servicio. Para obtener más información, consulte the section called “Roles vinculados a servicios”.

Para rotar el certificado del punto de enlace de un túnel de Site-to-Site VPN a través de la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de Site-to-Site VPN y, a continuación, elija Acciones, Modificar certificado de túnel de VPN.

4. Seleccione el punto de conexión del túnel.
5. Seleccione Save.

Para rotar el certificado del punto de enlace de un túnel de Site-to-Site VPN a través de la AWS CLI

Utilice el comando modify-vpn-tunnel-certificate.

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

Con la VPN de IP privada, puede implementar la VPN IPsec sobre Direct Connect, lo que permite cifrar el tráfico entre su red en las instalaciones y AWS, sin necesidad de utilizar direcciones IP públicas ni equipos de VPN adicionales de terceros.

Uno de los principales casos de uso de la VPN de IP privada sobre Direct Connect es ayudar a los clientes de los sectores financiero, sanitario y federal a cumplir los objetivos normativos y de cumplimiento. La VPN de IP privada a través de Direct Connect garantiza que el tráfico entre AWS y las redes en las instalaciones es seguro y privado, lo que permite a los clientes cumplir sus mandatos normativos y de seguridad.

Beneficios de la VPN de IP privada

- Administración y operaciones de red simplificadas: sin la VPN de IP privada, los clientes tienen que desplegar VPN y enrutadores de terceros para implementar las VPN privadas en las redes de Direct Connect. 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.
- Posición de seguridad mejorada: anteriormente, los clientes tenían que utilizar una interfaz virtual (VIF) pública de Direct Connect para cifrar el tráfico a través de Direct Connect, lo que requiere direcciones IP públicas para los puntos de conexión de la VPN. El uso de IP públicas aumenta la probabilidad de ataques externos (DOS), lo que a su vez obliga a los clientes a implementar equipos de seguridad adicionales para la protección de la red. Además, una VIF pública abre el acceso entre todos los servicios públicos de AWS y las redes de los clientes en las instalaciones, lo que aumenta la gravedad del riesgo. La característica de VPN de IP privada permite el cifrado a través de VIF de tránsito de Direct Connect (en lugar de VIF públicas), junto con la posibilidad de configurar IP públicas. Esto proporciona una conectividad privada de extremo a extremo, además del cifrado, lo que mejora la posición de seguridad general.

- Mayor escala de rutas: las conexiones VPN de IP privada ofrecen límites de rutas más altos (5000 rutas de salida y 1000 de entrada) en comparación con Direct Connect solamente, que en la actualidad tienen un límite de 200 rutas de salida y 100 de entrada.

Cómo funciona la VPN de IP privada

La IP privada de Site-to-Site VPN funciona sobre una interfaz virtual (VIF) de tránsito de Direct Connect. Utiliza una puerta de enlace de Direct Connect y otra de tránsito para interconectar sus redes en las instalaciones con las VPC de AWS. Una conexión de VPN de IP privada tiene puntos de terminación en la puerta de enlace de tránsito en AWS y en su dispositivo de puerta de enlace de cliente en las instalaciones. Debe asignar direcciones IP privadas a la puerta de enlace de tránsito y a los extremos del dispositivo de puerta de enlace de cliente de los túneles IPsec. Puede utilizar direcciones IP privadas de los rangos de direcciones IPv4 privadas RFC1918 o RFC6598.

Adjunta una conexión de VPN de IP privada a una puerta de enlace de tránsito. A continuación, enruta el tráfico entre la conexión de VPN y cualquier VPC (u otras redes) que también estén conectadas a la puerta de enlace de tránsito. Esto se hace asociando una tabla de enrutamiento con la conexión de VPN. En la dirección inversa, puede enrutar el tráfico de sus VPC a la conexión de VPN de IP privada mediante las tablas de enrutamiento que están asociadas a las VPC.

La tabla de enrutamiento asociada a la conexión de VPN puede ser la misma o distinta que la asociada a la conexión de Direct Connect subyacente. De esta forma, podrá enrutar simultáneamente el tráfico cifrado y no cifrado entre sus VPC y sus redes en las instalaciones.

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 Direct Connect.

Tareas

- Creación de una AWS Site-to-Site VPN de IP privada través de Direct Connect

Creación de una AWS Site-to-Site VPN de IP privada través de Direct Connect

Para crear una VPN de IP privada con Direct Connect siga 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 Site-to-Site VPN.	Cree la puerta de enlace de tránsito mediante la consola de 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 hub de tránsito de red que puede utilizar para interconectar sus VPC y redes en las instalaciones. 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 puerta de enlace de Direct Connect para Site-to-Site 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 Creación de una puerta de enlace de AWS Direct Connect en la Guía del usuario de Direct Connect.	Una puerta de enlace de Direct Connect le permite conectar interfaces virtuales (VIF) en varias regiones de AWS. Esta puerta de enlace se utiliza para conectarse a VIF.

Elemento	Pasos	Información
Cree la asociación de la puerta de enlace de tránsito para 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 desasociar Direct Connect con una puerta de enlace de tránsito en la Guía del usuario de Direct Connect.	Después de crear la puerta de enlace de Direct Connect, cree una asociación de puerta de enlace de tránsito para la puerta de enlace de Direct Connect. Especifique el CIDR de IP privada para la puerta de enlace de tránsito que se identificó anteriormente en la lista de prefijos permitidos.

Creación de la puerta de enlace de cliente y conexión para Site-to-Site VPN

Una puerta de enlace de cliente es un recurso que crea en AWS. Representa el dispositivo de puerta de enlace de cliente en las instalaciones. Cuando crea una gateway del cliente, proporciona información sobre el 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 privada de AWS AWS Site-to-Site VPN, debe especificar sus propias direcciones IP de punto de conexión del túnel mediante las direcciones RFC 1918. No utilice las direcciones IP punto a punto para la interconexión eBGP entre el router de la puerta de enlace de cliente y el punto de conexión de Direct Connect. AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de la puerta de enlace de cliente como dirección de origen o destino en lugar de conexiones punto a punto. 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, elija Conexiones de Site-to-Site VPN.
10. Elija Create VPN Connection (Crear conexión VPN).
11. (Opcional) En Name tag (Etiqueta de nombre), escriba el nombre de la conexión de 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 Túnel dentro de la versión IP, especifique si los túneles de VPN admiten tráfico IPv4 o IPv6.
16. (Opcional) Si especificó IPv4 para Túnel dentro de la versión IP, puede especificar opcionalmente los intervalos CIDR de IPv4 para la puerta de enlace de cliente y los lados de AWS que pueden comunicarse a través de los túneles de VPN. El valor predeterminado es `0.0.0.0/0`.

Si especificó IPv6 para Túnel dentro de la versión IP, puede especificar opcionalmente los intervalos CIDR de IPv6 para la puerta de enlace de cliente y los lados de AWS que tienen permiso para comunicarse a través de los túneles de VPN. El valor predeterminado para ambos rangos es `::/0`.

17. En Tipo de dirección IP externa, elija PrivateIpv4.
18. En Transport attachment ID (ID de conexión de transporte), elija la conexión de puerta de enlace de tránsito de la puerta de enlace de Direct Connect apropiada.
19. Elija Create VPN Connection (Crear conexión VPN).

> **Note**
>
> La opción Enable acceleration (Habilitar aceleración) no es aplicable a las conexiones de VPN sobre Direct Connect.

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

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

Seguridad en AWS Site-to-Site VPN

La seguridad en AWS es la principal prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida aborda tanto la seguridad de la nube como la seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS 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 Programas de conformidad de AWS. Para obtener información sobre los programas de conformidad que se aplican a AWSSite-to-Site VPN, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad está determinada por el servicio de AWS 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 comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Site-to-Site VPN. En los siguientes temas, se le mostrará cómo configurar Site-to-Site VPN para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros servicios de AWS que le ayudarán a monitorear y proteger los recursos de Site-to-Site VPN.

Contenido

Características de seguridad de AWS Site-to-Site VPN mejoradas con Secrets Manager

La característica Security Rebase de AWS Site-to-Site VPN proporciona capacidades de seguridad mejoradas que le brindan mayor control y visibilidad de sus conexiones de VPN. Una mejora clave es la capacidad de almacenar claves compartidas previamente (PSK) en AWS Secrets Manager en lugar de directamente en el servicio Site-to-Site VPN, lo que permite mejorar la administración de los secretos y el cumplimiento de las prácticas recomendadas de seguridad. La característica también incluye una API `GetActiveVpnTunnelStatus` que proporciona visibilidad en tiempo real de los parámetros de seguridad que se utilizan en los túneles de VPN activos, incluidos los algoritmos de cifrado, los algoritmos de integridad y los grupos de Diffie-Hellman para ambas fases de IKE. Además, ahora puede generar las configuraciones de seguridad recomendadas que imponen el uso de protocolos modernos excluyendo opciones antiguas como IKEv1. Estas mejoras resultan especialmente valiosas si su organización debe mantener estándares de seguridad estrictos, requiere registros de auditoría detallados de las configuraciones de VPN o desea asegurarse de que las conexiones de VPN utilizan los protocolos más seguros disponibles.

Contenido

Cambio de la clave compartida previamente de Secrets Manager en AWS Site-to-Site VPN

Si no se puede acceder a un túnel en Secrets Manager, puede cambiar la clave compartida previamente de dicho túnel.

> **Note**
>
> - Al cambiar la clave compartida previamente, asegúrese de tener los permisos de IAM necesarios para el servicio Secrets Manager.

- Tras cambiar la clave compartida previamente de un túnel de VPN, la conectividad se interrumpe durante varios minutos. Asegúrese de planificar el tiempo de inactividad esperado.

Para cambiar la clave compartida previamente de Secrets Manager para un túnel de VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de Site-to-Site VPN y elija Acciones, Modificar las opciones de túnel de VPN.
4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. En Nueva clave compartida previamente, elija una nueva clave compartida previamente.

> **Note**
>
> Esta opción solo está disponible para claves almacenadas en Secrets Manager.

6. Seleccione Save changes (Guardar cambios).
7. Repita estos pasos para cualquier otro túnel.

Cambio del modo de almacenamiento de claves compartidas previamente en AWS Site-to-Site VPN

Cambie el modo de almacenamiento de claves compartidas previamente para un túnel de 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 la clave compartida previamente de un túnel de VPN, la conectividad se interrumpe durante varios minutos. Asegúrese de planificar el tiempo de inactividad esperado.

Cómo cambiar el modo de almacenamiento de claves compartidas previamente

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones de Site-to-Site VPN.
3. Seleccione la conexión de Site-to-Site VPN y elija Acciones, Modificar las opciones de túnel de 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 compartidas previamente, elija uno de los siguientes tipos de almacenamiento de claves compartidas previamente.
   - Estándar: la clave compartida previamente se guarda directamente en el servicio Site-to-Site VPN.
   - Secrets Manager: la clave compartida previamente se almacena mediante AWS Secrets Manager. Para obtener más información acerca de Secrets Manager, consulte Características de seguridad mejoradas con Secrets Manager.
6. Seleccione Save changes (Guardar cambios).

Al cambiar el modo de almacenamiento de Secrets Manager a Estándar:

- La clave compartida previamente se elimina de Secrets Manager y se traslada al servicio Site-to-Site VPN.
- La entrada del túnel se elimina del secreto de Secrets Manager.

Al cambiar el modo de almacenamiento de Estándar a Secrets Manager:

- La clave compartida previamente se elimina del servicio Site-to-Site VPN.
- Se crea un nuevo secreto de Secrets Manager, si aún no existe uno.
- La nueva clave compartida previamente se almacena en Secrets Manager.

Protección de datos en AWS Site-to-Site VPN

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos de AWS Site-to-Site VPN. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la 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, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario 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.
- Utiliza SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulta Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utiliza las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de 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 FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utiliza un punto de conexión de 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 se trabaja con Site-to-Site VPN u otros Servicios de AWS con la consola, la API, la AWS CLI o los SDK de AWS. 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

Las conexiones de Site-to-Site VPN conectan 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 da soporte a conexiones de VPN de seguridad de protocolo de Internet (IPSec). IPsec es un conjunto de protocolos que se usa para proteger las comunicaciones por protocolo de Internet (IP) mediante la autenticación y el cifrado de todos los paquetes IP de una transmisión de datos.

Cada conexión de Site-to-Site VPN consta de dos túneles de VPN IPsec cifrados que conectan AWS y la red. El tráfico de cada túnel puede cifrarse con AES128 o AES256 y usar grupos Diffie-Hellman para el intercambio de claves, lo que proporciona una confidencialidad directa total. AWS autentica con funciones de hash SHA1 o SHA2.

Las instancias de la VPC no necesitan una dirección IP pública para conectarse a los recursos del otro extremo de la conexión de Site-to-Site VPN. Las instancias pueden direccionar el tráfico de Internet hacia la red de las instalaciones a través de la conexión de Site-to-Site VPN. 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 la conexión de AWS Site-to-Site VPN: proporciona información sobre las opciones de IPsec e Intercambio de claves de Internet (IKE) disponibles para cada túnel.
- AWS Site-to-Site VPNOpciones de autenticación de túneles de : proporciona información sobre las opciones de autenticación de los puntos de enlace del túnel de VPN.
- Requisitos para un dispositivo de puerta de enlace de cliente de AWS Site-to-Site VPN: proporciona información sobre los requisitos del dispositivo de gateway de cliente en su extremo de la conexión de VPN.
- Comunicación segura entre conexiones de AWS Site-to-Site VPN mediante VPN CloudHub: si tiene varias conexiones de Site-to-Site VPN, puede proporcionar una comunicación segura entre los sitios en las instalaciones con AWS VPN CloudHub.

Administración de identidades y accesos de AWS Site-to-Site VPN

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los gestionadores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Site-to-Site VPN. IAM es un servicio de Servicio de AWS que se puedes utilizar sin cargo adicional.

Temas

Público

Cómo el uso de AWS Identity and Access Management (IAM) varía en función del rol:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte Solución de problemas de identidades y accesos en AWS Site-to-Site VPN)
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte Funcionamiento de AWS Site-to-Site VPN con IAM)
- Administrador de IAM: escriba políticas para administrar el acceso (consulte Ejemplos de políticas basadas en identidad para AWS Site-to-Site VPN)

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión como una identidad federada con credenciales de un origen de identidad como AWS IAM Identity Center (IAM Identity Center), autenticación de inicio de sesión único o credenciales

de Google/Facebook. Para obtener más información sobre el inicio de sesión, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Para el acceso programático, AWS proporciona un SDK y una CLI para firmar criptográficamente las solicitudes. Para obtener más información, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Usuario raíz de la Cuenta de AWS

Cuando crea una Cuenta de AWS, comienza con una identidad de inicio de sesión denominada usuario raíz de la Cuenta de AWS, que tiene acceso completo a todos los Servicios de AWS y recursos. Recomendamos encarecidamente que no utilice el usuario raíz para las tareas diarias. Para ver las tareas que requieren credenciales de usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, exija a los usuarios humanos que utilicen la federación con un proveedor de identidades para acceder a Servicios de AWS con credenciales temporales.

Una identidad federada es un usuario de su directorio empresarial, proveedor de identidad web o Directory Service que accede a los Servicios de AWS mediante credenciales de un origen de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, recomendamos AWS IAM Identity Center. Para obtener más información, consulte ¿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 con permisos específicos para una sola persona o aplicación. Recomendamos utilizar credenciales temporales en lugar de usuarios de IAM con credenciales a largo plazo. Para obtener más información, consulte Solicitar que los usuarios humanos utilicen la federación con un proveedor de identidades para acceder a AWS mediante credenciales temporales en la Guía del usuario de IAM.

Un grupo de IAM especifica una colección de usuarios de IAM y facilita la administración de los permisos para grandes conjuntos de usuarios. 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 con permisos específicos que proporciona credenciales temporales. Puede asumir un rol cambiando de usuario a un rol de IAM (consola) o llamando a una operación de la API o la AWS CLI de AWS. Para obtener más información, consulte Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM son útiles para el acceso de usuarios federados, los permisos de usuario de IAM temporales, el acceso entre cuentas, el acceso entre servicios y las aplicaciones que se ejecutan en Amazon EC2. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política define los permisos cuando se asocia a una identidad o un recurso. AWS evalúa estas políticas cuando una entidad principal realiza una solicitud. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre los documentos de políticas JSON, consulte Información general de políticas JSON en la Guía del usuario de IAM.

Mediante las políticas, los administradores especifican quién tiene acceso a qué, definiendo qué entidad principal puede realizar acciones sobre qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un administrador de IAM crea políticas de IAM y las añade a los roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método utilizado para realizar la operación.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede asociar a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, sobre 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 identidad pueden ser políticas insertadas (incrustadas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener más información sobre cómo elegir entre políticas administradas o políticas insertadas, consulte Selección 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 políticas JSON que se asocian a un recurso. Algunos ejemplos 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. Debe especificar una entidad principal en una política en función de recursos.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer el máximo de permisos concedidos por los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en la identidad puede conceder a una entidad de IAM. Para obtener más información, consulte Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.
- Políticas de control de servicios (SCP): especifican los permisos máximos para una organización o unidad organizativa en AWS Organizations. Para obtener más información, consulte Políticas de control de servicios en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): establecen los permisos máximos disponibles para los recursos de las cuentas. Para obtener más información, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal para un rol o un usuario federado. 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 obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Funcionamiento de AWS Site-to-Site VPN con IAM

Antes de utilizar IAM para administrar el acceso a Site-to-Site VPN, conozca qué características de IAM se pueden utilizar con Site-to-Site VPN.

Funciones de IAM que puede utilizar con AWS Site-to-Site VPN

Característica de IAM	Compatibilidad con Site-to-Site 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
ACL	No
ABAC (etiquetas en políticas)	No
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	Sí

Para obtener una perspectiva general sobre cómo funcionan Site-to-Site VPN y otros servicios de AWS con las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas basadas en identidad para Site-to-Site VPN

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. 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 basadas en identidad para Site-to-Site VPN

Para ver ejemplos de políticas basadas en identidad de Site-to-Site VPN, consulte Ejemplos de políticas basadas en identidad para AWS Site-to-Site VPN.

Políticas basadas en recursos dentro de Site-to-Site VPN

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. Las entidades principales pueden incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Para obtener más información, consulte Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.

Acciones de política para Site-to-Site VPN

Compatibilidad con las acciones de políticas: sí

Los administradores pueden utilizar las políticas JSON de AWS 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. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de Site-to-Site VPN, consulte Acciones definidas por AWS Site-to-Site VPN en la Referencia de autorizaciones de servicio.

Las acciones de políticas en 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 basadas en identidad de Site-to-Site VPN, consulte Ejemplos de políticas basadas en identidad para AWS Site-to-Site VPN.

Recursos de políticas para Site-to-Site VPN

Compatibilidad con los recursos de políticas: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede 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. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Para las acciones que no admiten permisos por recurso, utilice 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 ARN, consulte Recursos definidos por AWS Site-to-Site VPN en la Referencia de autorizaciones de servicio. Para obtener información sobre las acciones con las que puede especificar el ARN de cada recurso, consulte Acciones definidas por AWS Site-to-Site VPN.

Para ver ejemplos de políticas basadas en identidad de Site-to-Site VPN, consulte Ejemplos de políticas basadas en identidad para AWS Site-to-Site VPN.

Claves de condición de política para Site-to-Site VPN

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. 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. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de Site-to-Site VPN, consulte Claves de condición para AWS Site-to-Site VPN en la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte Acciones definidas por AWS Site-to-Site VPN.

Para ver ejemplos de políticas basadas en identidad de Site-to-Site VPN, consulte Ejemplos de políticas basadas en identidad para AWS Site-to-Site VPN.

ACL en Site-to-Site VPN

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con Site-to-Site VPN

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 denominados etiquetas. Puede asociar etiquetas a entidades de IAM y recursos de AWS y, a continuación, diseñar políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso.

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 Site-to-Site VPN

Compatibilidad con credenciales temporales: sí

Las credenciales temporales proporcionan acceso a corto plazo a los recursos de AWS y se crean automáticamente cuando se utiliza la federación o se cambia de rol. AWS recomienda que genere de forma dinámica credenciales temporales en lugar de usar claves de acceso a largo plazo. Para obtener más información, consulte Credenciales de seguridad temporales en IAM y Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Permisos de entidades principales entre servicios para Site-to-Site VPN

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.

Roles de servicio para 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 Site-to-Site VPN. Edite los roles de servicio solo cuando Site-to-Site VPN proporcione orientación para hacerlo.

Roles vinculados a servicios para Site-to-Site VPN

Admite roles vinculados a servicios: sí

Un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la 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 basadas en identidad para AWS Site-to-Site VPN

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar recursos de Site-to-Site VPN. Un administrador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan.

Para obtener información acerca de cómo crear una política basada en identidad de IAM utilizando 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 Site-to-Site VPN, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS Site-to-Site VPN en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Site-to-Site VPN

- Descripción de conexiones de Site-to-Site VPN específicas
- Creación y descripción de los recursos necesarios para una conexión de AWS Site-to-Site VPN

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear, acceder o eliminar los recursos de Site-to-Site VPN de la cuenta. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comienza con las políticas administradas por AWSy continúa con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de tarea, utiliza las políticas administradas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas gestionadas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte 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, consulte 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, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, CloudFormation. Para obtener más información, consulte 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.

- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesite usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para obtener una 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 de Site-to-Site VPN

Para acceder a la consola de AWS Site-to-Site VPN, debe tener un mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de Site-to-Site VPN en su 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 conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la consola de Site-to-Site VPN, asocie el `AmazonVPCFullAccess` de Site-to-Site VPN o la política administrada `AmazonVPCReadOnlyAccess` AWS a las entidades. Para obtener más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Descripción de conexiones de Site-to-Site VPN específicas

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ec2:DescribeVpnConnections"
         ],
         "Resource": ["*"]
      }
```

```
   ]
}
```

Creación y descripción de los recursos necesarios para una conexión de AWS Site-to-Site VPN

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
         "ec2:DescribeVpnConnections",
         "ec2:DescribeVpnGateways",
         "ec2:DescribeCustomerGateways",
         "ec2:CreateCustomerGateway",
         "ec2:CreateVpnGateway",
         "ec2:CreateVpnConnection"
         ],
         "Resource": [
            "*"
         ]
      },
   {
         "Effect": "Allow",
         "Action": "iam:CreateServiceLinkedRole",
         "Resource": "arn:aws:iam::*:role/aws-service-role/s2svpn.amazonaws.com/
AWSServiceRoleForVPCS2SVPNInternal",
         "Condition": {
            "StringLike": {
               "iam:AWSServiceName":"s2svpn.amazonaws.com"
            }
         }
      }
   ]
}
```

Solución de problemas de identidades y accesos en AWS Site-to-Site VPN

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Site-to-Site VPN e IAM.

Temas

No tengo autorización para realizar una acción en Site-to-Site VPN

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 gestionador de AWS. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, las políticas deben actualizarse a fin de permitirle pasar un rol a Site-to-Site VPN.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Site-to-Site VPN. 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 gestionador de AWS. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso 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 admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Site-to-Site VPN admite estas características, consulte Funcionamiento de AWS Site-to-Site VPN con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Acceso para un usuario de IAM en otra Cuenta de AWS propia en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulta Proporcionar acceso a Cuentas de AWS que 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.

políticas administradas de AWS para Site-to-Site VPN

Para agregar permisos a usuarios, grupos y roles, es más fácil utilizar las políticas administradas de AWS que escribirlas uno mismo. Se necesita tiempo y experiencia para crear políticas administradas por el cliente de IAM que le brinden a su equipo solo los permisos necesarios. Para comenzar a hacerlo con rapidez, puede utilizar nuestras políticas administradas de AWS. Estas políticas cubren casos de uso comunes y están disponibles en su cuenta de AWS. Para obtener más información sobre las políticas administradas de AWS, consulte Políticas administradas de AWS en la Guía del usuario de IAM.

Los servicios de AWS mantienen y actualizan las políticas administradas de AWS. No puede cambiar los permisos en las políticas gestionadas de AWS. 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 administrada de AWScuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no quitan los permisos de una política administrada de AWS, por lo tanto, las actualizaciones de las políticas no deteriorarán los permisos existentes.

Además, AWS admite políticas administradas para funciones de trabajo que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` administrada por AWS proporciona acceso de solo lectura a todos los servicios y recursos de AWS. Cuando un servicio lanza una nueva característica, AWS agrega permisos de solo lectura para las operaciones y los recursos nuevos. 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.

política administrada de AWS: AWSVPCS2SVpnServiceRolePolicy

Puede adjuntar la política `AWSVPCS2SVpnServiceRolePolicy` a las identidades de IAM. Esta política permite a Site-to-Site VPN administrar un secreto de AWS Secrets Manager en 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.

Actualizaciones de las políticas administradas de AWS en Site-to-Site VPN

Consulte los detalles sobre las actualizaciones de las políticas administradas de AWS para Site-to-Site VPN desde que este servicio comenzó a realizar un seguimiento de estos cambios en mayo de 2025.

Cambio	Descripción	Fecha
AWSVPCS2SVpnServiceRolePolicy: política actualizada	Se han añadido nuevos permisos a la política que permiten a Site-to-Site VPN administrar el secreto administrado por `s2svpn` de AWS Secrets Manager de la conexión de VPN.	14 de mayo de 2025

Uso de roles vinculados a servicios para Site-to-Site VPN

AWS Site-to-Site VPN usa roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a un Site-to-Site VPN. Los roles vinculados a servicios están predefinidos por Site-to-Site VPN e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS en su nombre.

Un rol vinculado a servicios simplifica la configuración de Site-to-Site VPN porque ya no tendrá que añadir manualmente los permisos necesarios. Site-to-Site VPN define los permisos de sus roles vinculados a servicios y, a menos que esté definido de otra manera, solo Site-to-Site VPN puede asumir sus roles. 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. De esta forma, se protegen los recursos de Site-to-Site VPN, ya que se evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Rol vinculado a servicios para Site-to-Site VPN

Site-to-Site VPN utiliza el rol vinculado a servicios denominado AWSServiceRoleForVPCS2SVPN: permite a Site-to-Site VPN crear y gestionar recursos relacionados con las conexiones de su VPN.

El rol vinculado a servicios AWSServiceRoleForVPCS2SVPN depende del siguiente servicio para asumir el rol:

- `s2svpn.amazonaws.com`

El rol vinculado a servicios utiliza la política administrada AWSVPCS2SVpnServiceRolePolicy para realizar las siguientes acciones en los recursos especificados:

- Al utilizar la autenticación de certificados para la conexión de VPN, AWS Site-to-Site VPN exporta los certificados de AWS Certificate Manager del túnel de VPN para usarlos en los puntos de conexión del túnel de VPN.
- Al utilizar la autenticación de certificados para la conexión de VPN, AWS Site-to-Site VPN administra la renovación de los certificados de AWS Certificate Manager del túnel de VPN.
- Al utilizar el almacenamiento de claves compartidas previamente de SecretsManager para la conexión de VPN, AWS Site-to-Site VPN administra el secreto administrado s2svpn de AWS Secrets Manager de la conexión de VPN.

Para ver los permisos de esta política, consulte AWSVPCS2SVpnServiceRolePolicy en la Referencia de la política administrada de AWS.

Creación del rol vinculado a servicios para Site-to-Site VPN

No necesita crear manualmente un rol vinculado a servicios. Al crear una puerta de enlace de cliente con un certificado privado de ACM asociado en la Consola de administración de AWS, la AWS CLI o la API de AWS, Site-to-Site VPN crea el rol vinculado a servicios por usted.

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 puerta de enlace de cliente con un certificado privado de ACM asociado, Site-to-Site VPN crea el rol vinculado a servicios por usted de nuevo.

Edición de un rol vinculado a servicios para Site-to-Site VPN

Site-to-Site VPN no permite editar el rol vinculado a servicios AWSServiceRoleForVPCS2SVPN. 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.

Eliminación de un rol vinculado a servicios para Site-to-Site VPN

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 Site-to-Site VPN está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Site-to-Site VPN utilizados por el rol AWSServiceRoleForVPCS2SVPN

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. De esta manera, evitará eliminar por error el permiso para acceder a los certificados de ACM que se utilizan en las conexiones de Site-to-Site VPN.

Para eliminar manualmente el rol vinculado a un servicio mediante IAM

Utilice la consola de IAM, la AWS CLI o la API de AWS para eliminar el rol vinculado a servicios AWSServiceRoleForVPCS2SVPN. 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 global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. 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 centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, Site-to-Site VPN cuenta con varias características que lo ayudan a dar respuesta a sus necesidades de resiliencia y copia de seguridad de los datos.

Dos túneles por conexión de VPN

Una conexión de 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 su VPC. Si se produce un error del dispositivo en AWS, su conexión de VPN cambiará automáticamente al segundo túnel para que su acceso no se vea interrumpido. Cada cierto tiempo, AWS también lleva a cabo un mantenimiento rutinario en la conexión de VPN, lo que podría desactivar uno de los dos túneles de dicha conexión durante un breve periodo. Para obtener más información, consulte reemplazos de los puntos de conexión de un túnel de AWS Site-to-Site VPN. Al configurar su gateway de cliente, por tanto es importante que configure ambos túneles.

Redundancia

Para protegerse contra una eventual pérdida de conectividad en caso de que la gateway de cliente dejara de estar disponible, puede configurar otra conexión de Site-to-Site VPN. Para obtener más información, consulte la documentación siguiente:

- Conexiones de AWS Site-to-Site VPN redundantes para conmutación por error
- Opciones de conectividad de Amazon Virtual Private Cloud
- Creación de una infraestructura de red de AWS multiVPC escalable y segura

Seguridad de la infraestructura en AWS Site-to-Site VPN

Como se trata de un servicio administrado, AWS Site-to-Site VPN está protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS siguiendo las prácticas recomendadas de seguridad de infraestructura, consulte Protección de la infraestructura en Portal de seguridad de AWS Well-Architected Framework.

Utilice las llamadas a las API publicadas de AWS para acceder a 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.

Supervisión de una conexión de AWS Site-to-Site VPN

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el desempeño de su conexión de AWS Site-to-Site VPN. 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. No obstante, antes de comenzar a monitorear la conexión de Site-to-Site VPN, debe crear un plan que responda a las siguientes preguntas:

- ¿Cuáles son los objetivos de la monitorización?
- ¿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 dispone de diversas herramientas que puede utilizar para monitorear una conexión de 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 monitoreo automatizadas

Puede utilizar las siguientes herramientas de monitoreo automatizado para vigilar las conexiones de Site-to-Site VPN e informar cuando haya algún problema:

- Alarmas de Amazon CloudWatch: vigile una métrica durante un periodo de tiempo especificado y realice una o varias acciones según el valor que tenga la métrica en comparación con un determinado umbral durante una serie de periodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. Las alarmas de CloudWatch no invocan acciones tan solo por tener un estado determinado; es necesario que el estado haya cambiado y se mantenga durante un número específico de periodos. Para obtener más información, consulte Supervisión de túneles de AWS Site-to-Site VPN con Amazon CloudWatch.
- Supervisión de registros de AWS CloudTrail: comparta archivos de registro entre cuentas, supervise los archivos de registro de CloudTrail en tiempo real enviándolos a CloudWatch Logs, escriba aplicaciones de procesamiento de registros en Java y compruebe que los archivos de registro no hayan cambiado después de que CloudTrail los entregara. Para obtener más información, consulte Registro de las llamadas a la API mediante AWS CloudTrail en la Referencia de la API de Amazon EC2 y Uso de archivos de registro de CloudTrail en la Guía del usuario de AWS CloudTrail.
- Eventos de AWS Health: reciba alertas y notificaciones relacionadas con los cambios de estado de los túneles de Site-to-Site VPN, recomendaciones de configuración de prácticas recomendadas o cuando se aproxime 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 Eventos de AWS Health y AWS Site-to-Site VPN.

Herramientas de monitoreo manuales

Otra factor importante del monitoreo de conexiones de Site-to-Site VPN implica el control manual de los elementos que no cubren las alarmas de CloudWatch. Los paneles de las consolas de Amazon VPC y CloudWatch proporcionan una vista rápida del estado del entorno de AWS.

> **Note**
>
> En la consola de Amazon VPC, es posible que los parámetros de estado del túnel de 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 las métricas y los registros de CloudWatch para las actualizaciones granulares de los cambios de estado de los túneles.

- En el panel de control de Amazon VPC se indica:
  - El estado de los servicios en cada región
  - Las conexiones de Site-to-Site VPN
  - El estado del túnel de VPN: en el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN), seleccione una conexión de Site-to-Site VPN y haga clic en Tunnel Details (Detalles del túnel)
- La página principal de CloudWatch muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede utilizar CloudWatch para 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
  - Buscar y examinar todas sus métricas de recursos de AWS.
  - Crear y editar las alarmas de notificación de problemas

AWS Site-to-Site VPNRegistros de

Los registros de AWS Site-to-Site VPN le proporcionan una mayor visibilidad de las implementaciones de Site-to-Site VPN. Con esta característica, tiene acceso a los registros de conexión de Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones de intercambio de claves de Internet (IKE) y los mensajes del protocolo de detección de pares muertos (DPD).

Los registros de Site-to-Site VPN se pueden publicar en registros de Amazon CloudWatch. Esta característica proporciona a los clientes una única forma coherente de acceder y analizar registros detallados para todas las conexiones de Site-to-Site VPN.

Temas

Beneficios de los registros de Site-to-Site VPN

- Solución de problemas de VPN simplificada: los registros de Site-to-Site VPN le ayudan a identificar desajustes de configuración entre AWS y el dispositivo de puerta de enlace de cliente y abordar los problemas iniciales de conectividad de 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.
- Visibilidad de AWS Site-to-Site VPN centralizada: los registros de Site-to-Site VPN pueden proporcionar registros de actividad de túnel para todas las diferentes formas en que se conecta Site-to-Site VPN: puerta de enlace virtual, puerta de enlace de tránsito y CloudHub, con Internet

y Direct Connect como transporte. Esta característica proporciona a los clientes una única forma coherente de acceder y analizar registros detallados para todas las conexiones Site-to-Site VPN.

- Seguridad y conformidad: los registros de Site-to-Site VPN se pueden enviar a registros de Amazon CloudWatch para realizar un análisis retrospectivo del estado y la actividad de la conexión de VPN a lo largo del tiempo. Esto puede ayudarle a cumplir con los requisitos reglamentarios y de conformidad.

Restricciones de tamaño de política de recursos de registros de Amazon CloudWatch

Las políticas de recursos de Registros de Amazon CloudWatch están limitadas a 5120 caracteres. Cuando Registros de Amazon CloudWatch detecta que una política se acerca a este límite de tamaño, habilita automáticamente los grupos de registro que comienzan con `/aws/vendedlogs/`. Al habilitar el registro, Site-to-Site VPN debe actualizar la política de recursos de Registros de Amazon CloudWatch con el grupo de registro que especifique. Para evitar alcanzar el límite de tamaño de la política de recursos de Registros de Amazon CloudWatch, ponga el prefijo a los nombres del grupo de registro con `/aws/vendedlogs/`.

Contenido del registro de Site-to-Site VPN

La siguiente información se incluye en el registro de actividad de túnel de Site-to-Site VPN. El nombre del archivo de flujo de registro utiliza VpnConnectionID y TunnelOutsideIPAddress.

Campo	Descripción
VpnLogCreationTimestamp (`event_timestamp`)	Marca temporal de creación de registros en formato legible por humanos.
TunnelDPDEnabled (`dpd_enabled`)	Estado habilitado del protocolo de detección de pares muertos (verdadero/falso).
TunnelCGWNATTDetectionStatus (`nat_t_detected`)	NAT-T detectado en el dispositivo de puerta de enlace de cliente (verdadero/falso).
TunnelIKEPhase1State (`ike_phase1_state`)	Estado del protocolo de fase 1 de IKE (Establecido | Cambio de clave | Negociación | Inactivo).

Campo	Descripción
TunnelIKEPhase2State (`ike_phase2_state`)	Estado del protocolo de fase 2 de IKE (Establecido | Cambio de clave | Negociación | Inactivo).
VpnLogDetail (`details`)	Mensajes detallados para los protocolos IPsec, IKE y DPD.

Contenido

Mensajes de error de IKEv1

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.
El descifrado de la carga del túnel de AWS no se ha realizado correctamente debido a la clave previamente compartida no válida	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.
No se encontró ninguna coincidencia de propuesta de 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.

Mensaje	Explicación
El túnel de AWS recibió DELETE para la fase 2 SA con SPI: xxxx	CGW ha enviado el mensaje Delete_SA para la fase 2.
El túnel de AWS recibió DELETE para IKE_SA de CGW	CGW ha enviado el mensaje Delete_SA para la fase 1.

Mensajes de error de IKEv2

Mensaje	Explicación
Se agotó el tiempo de espera del DPD del túnel de AWS después de que {retry_count} retransmita	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
El túnel de AWS recibió DELETE para IKE_SA de CGW	El par ha enviado el mensaje Delete_SA para Parent/IKE_SA.
El túnel de AWS recibió DELETE para la fase 2 SA con SPI: xxxx	El par ha enviado el mensaje Delete_SA para CHILD_SA.
El túnel de AWS detectó una colisión (CHILD_REKEY) como CHILD_DELETE	CGW ha enviado el mensaje Delete_SA para la SA activa, a la que se le está cambiando la clave.
Se está eliminando la SA redundante del túnel de AWS (CHILD_SA) debido a la colisión detectada	Debido a una colisión, si se generan SA redundantes, los pares cerrarán la SA redundante después de hacer coincidir los valores nonce según RFC.
La fase 2 del túnel de AWS no se pudo establecer 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

Mensaje	Explicación
	se deben configurar con CIDR idénticos y correctos.
El túnel de AWS envía AUTHENTICATION_FAILED como respuesta	El par no puede autenticar al par al verificar el contenido del mensaje IKE_AUTH
El túnel de AWS detectó una discrepancia de clave previamente compartida con cgw: xxxx	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.
Tiempo de espera del túnel de AWS: eliminación de 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 coincidencia de propuesta de AWS	El punto de conexión de AWS VPN no admite los atributos propuestos para la fase 1 o la fase 2 (cifrado, hash y grupo DH), por ejemplo, `3DES`.

Mensajes de negociación de IKEv2

Mensaje	Explicación
El túnel de AWS ha procesado una solicitud (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la solicitud CREATE_CHILD_SA de CGW.
El túnel de AWS envía una respuesta (id=xxx) para CREATE_CHILD_SA	AWS envía una respuesta CREATE_CHILD_SA a CGW.
El túnel de AWS envía una solicitud (id=xxx) para CREATE_CHILD_SA	AWS envía una solicitud CREATE_CHILD_SA a CGW.

Mensaje	Explicación
El túnel de AWS ha procesado una respuesta (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la respuesta CREATE_CHILD_SA de CGW.

Requisitos de IAM para publicar en CloudWatch Logs

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 puede encontrar más detalles en la sección Habilitar el registro desde determinados servicios de AWS de la Guía del usuario de Registros de Amazon CloudWatch.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogDelivery",
        "logs:GetLogDelivery",
        "logs:UpdateLogDelivery",
        "logs:DeleteLogDelivery",
        "logs:ListLogDeliveries"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow",
      "Sid": "S2SVPNLogging"
    },
    {
      "Sid": "S2SVPNLoggingCWL",
      "Action": [
        "logs:PutResourcePolicy",
        "logs:DescribeResourcePolicies",
        "logs:DescribeLogGroups"
      ],
      "Resource": [
```

```
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

Visualización de la configuración de los registros de AWS Site-to-Site VPN

Consulte el registro de actividades de una conexión de 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, elija Conexiones de 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 consultar el estado actual de la característica de registro en Tunnel VPN log (Registro de VPN de túnel) y el grupo de registro de CloudWatch configurado actualmente (si lo hay) en CloudWatch log group (Grupo de registro de CloudWatch).

Para consultar la configuración actual de registro de túnel en una conexión de Site-to-Site VPN con la línea de comandos de AWS o la API

- DescribeVpnConnections (API de consulta de Amazon EC2)
- describe-vpn-connections (AWS CLI)

Habilitación de registros de AWS Site-to-Site VPN

Habilite los registros de Site-to-Site VPN para registrar la actividad de 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 Desactivar registros de Site-to-Site VPN.

> **Note**
>
> Cuando habilita los registros de Site-to-Site VPN para un túnel de conexión de VPN existente, la conectividad a través de ese túnel se puede interrumpir 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 reemplazos de los puntos de conexión de un túnel de AWS Site-to-Site VPN.

Para habilitar el registro de VPN durante la creación de una nueva conexión de 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 la conexión de AWS Site-to-Site VPN.

Para habilitar el registro de túnel en una conexión de Site-to-Site VPN nueva con la línea de comandos de AWS o la API

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

Para habilitar el registro de túnel en una conexión de 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, elija Conexiones de 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 Amazon CloudWatch log group (Grupo de registros de Amazon CloudWatch), seleccione el grupo de registros de Amazon CloudWatch al que desea 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 túnel en una conexión de Site-to-Site VPN existente con la línea de comandos de AWS o la API

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

Desactivación de los registros de AWS Site-to-Site VPN

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 Habilitar registros de Site-to-Site VPN.

Para desactivar el registro de túnel en una conexión de 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 (Conexiones de 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), 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 desactivar el registro de túnel en una conexión de Site-to-Site VPN con la línea de comandos de AWS o la API

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

Supervisión de túneles de AWS Site-to-Site VPN con Amazon CloudWatch

Puede monitorear los túneles de VPN utilizando CloudWatch, que recopila y procesa los datos sin formato del servicio VPN en métricas legibles y casi 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 VPN se envían automáticamente a CloudWatch en cuanto están disponibles.

Para obtener más información, consulte la Guía del usuario de Amazon CloudWatch.

Contenido

Dimensiones y métricas de VPN

Las siguientes métricas de CloudWatch están disponibles para las conexiones de VPN de sitio a sitio.

Métrica	Descripción
`TunnelState`	El estado de los túneles. Para las VPN estáticas, 0 indica DOWN y 1 indica UP. Para las VPN de BGP, 1 indica ESTABLISHED y 0 se utiliza para los demás estados. Para los dos

Métrica	Descripción
	tipos de VPN, los valores entre 0 y 1 indican que al menos que un túnel no es UP. Unidades: valor fraccional entre 0 y 1
`TunnelDataIn` †	Los bytes recibidos en el lado de AWS de la conexión a través del túnel de VPN desde una gateway 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 lado de AWS de la conexión a través del túnel de VPN a una gateway de 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 de las métricas por el ID de Site-to-Site VPN.
`TunnelIpAddress`	Filtra los datos de las métricas en función de la dirección IP del túnel de la gateway privada virtual.

Visualización de las métricas de Registros de Amazon CloudWatch para AWS Site-to-Site VPN

Cuando se crea una conexión de VPN de sitio a sitio, el servicio de VPN envía métricas sobre la conexión de VPN a CloudWatch en cuanto están disponibles. Puede ver las métricas de la conexión de VPN de la siguiente manera.

Para ver las métricas a través de la consola de CloudWatch

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 consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, seleccione Metrics (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 consola de CloudWatch hasta que se haya creado una conexión de VPN de sitio a sitio en la región de AWS que está viendo.

Para ver métricas mediante la AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

```
aws cloudwatch list-metrics --namespace "AWS/VPN"
```

Creación de alarmas de Amazon CloudWatch para supervisar los túneles de AWS Site-to-Site VPN

Puede crear una alarma de CloudWatch que envíe un mensaje de Amazon SNS cuando la alarma cambia 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 consola de CloudWatch 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 métrica TunnelState. Elija Seleccionar métrica.
6. Para Siempre que TunnelState esté..., seleccione Inferior y, a continuación, escriba “1” en el campo de entrada en que... .
7. En Configuración adicional, establezca las entradas en “3 de 3” para los Puntos de datos para la alarma.
8. Elija Siguiente.
9. En Enviar una notificación al siguiente tema de SNS, seleccione una lista de notificación existente o cree una nueva.
10. Elija Siguiente.
11. Escriba un nombre para la alarma. Seleccione Siguiente.
12. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Puede crear una alarma que monitoree el estado de la conexión de 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.

Si desea crear una alarma para el estado de la conexión de Site-to-Site VPN

1. Abra la consola de CloudWatch 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 la conexión de Site-to-Site VPN y la métrica TunnelState . Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Maximum (Máximo).

   Si ha configurado la conexión de Site-to-Site VPN de modo que ambos túneles estén activos, también puede especificar la estadística Minimum (Mínima) para que se envíe una notificación cuando haya al menos un túnel inactivo.
7. En Siempre, elija Menor o igual que (<=) e introduzca 0 (o 0,5 cuando hay al menos un túnel desactivado). Seleccione 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. Seleccione Siguiente.
9. Escriba un nombre y la descripción de su alarma. Seleccione 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. Abra la consola de CloudWatch 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 de VPN y la métrica TunnelDataIn. 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. Seleccione 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. Seleccione Siguiente.
10. Escriba un nombre y la descripción de su alarma. Seleccione 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 consola de CloudWatch 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 de VPN y la métrica TunnelDataOut. 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`. Seleccione 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. Seleccione Siguiente.
10. Escriba un nombre y la descripción de su alarma. Seleccione Siguiente.
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Para obtener más ejemplos sobre la creación de alarmas, consulte este artículo acerca de cómo crear alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Eventos de AWS Health y AWS Site-to-Site VPN

AWS Site-to-Site VPN envía automáticamente notificaciones a AWS Health Dashboard. El panel no requiere instalación y está listo para que lo utilicen los usuarios de AWS autenticados. Puede configurar varias acciones en respuesta a las notificaciones de eventos a través de AWS Health Dashboard.

AWS Health Dashboard dispone de los siguientes tipos de notificaciones para las conexiones de 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 de punto de enlace en un túnel en AWS Health Dashboard cuando uno o ambos puntos de enlace de un túnel de VPN sea reemplazado en su conexión de 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 reemplazos de los puntos de conexión de un túnel de AWS Site-to-Site VPN.

Cuando se completa la sustitución de un punto de enlace de un túnel, AWS envía la notificación de sustitución del punto de enlace de un túnel a través de un evento de AWS Health Dashboard.

Notificaciones de VPN con un solo túnel

Por motivos de redundancia, las conexiones de Site-to-Site VPN tienen dos túneles. 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 VPNCuotas de

Su cuenta de AWS tiene las siguientes cuotas, anteriormente conocidas como límites, relacionadas con Site-to-Site VPN. A menos que se indique otra cosa, cada cuota es específica de la región. 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 este tema acerca de cómo solicitar un aumento de cuota en la Guía del usuario de Service Quotas.

Recursos de Site-to-Site VPN

Nombre	Valor predeterminado	Ajustable
Gateways de cliente por región	50	Sí
Gateways privadas virtuales por región	5	Sí
Conexiones de Site-to-Site VPN por región	50	Sí
Conexiones de Site-to-Site VPN por gateway privada virtual	10	Sí
Conexiones de Site-to-Site VPN aceleradas por región	10	Sí
Conexiones de Site-to-Site VPN no asociadas por región	10	Sí

> **Note**
>
> Tanto las conexiones aceleradas como las no asociadas se tienen en cuenta en la cuota total de conexiones de Site-to-Site VPN por región.

Puede asociar una gateway privada virtual a una VPC a la vez. Para establecer la misma conexión de Site-to-Site VPN con varias VPC, le recomendamos que valore la posibilidad de utilizar una

gateway de tránsito en su lugar. Para obtener más información, consulte Gateways de tránsito en Gateways de tránsito de Amazon VPC.

Las conexiones de Site-to-Site VPN en una gateway de tránsito están sujetas al límite total de las conexiones de gateway 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 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 entre un dispositivo de gateway de cliente y una conexión de Site-to-Site VPN de una gateway privada virtual	100	No
Rutas anunciadas entre una conexión de Site-to-Site VPN de una gateway privada virtual y un dispositivo de gateway de cliente	1 000	No
Rutas dinámicas anunciadas entre un dispositivo de gateway de cliente y una conexión de Site-to-Site VPN en una gateway de tránsito	1 000	No

Nombre	Valor predeterminado	Ajustable
Rutas anunciadas entre una conexión de Site-to-Site VPN de una gateway de tránsito y un dispositivo de gateway de cliente	5 000	No
Rutas estáticas entre un dispositivo de puerta de enlace de cliente y una conexión de Site-to-Site VPN en una puerta de enlace privada virtual	100	No

Ancho de banda y rendimiento

Hay muchos factores que pueden afectar el ancho de banda obtenido a través de una conexión Site-to-Site VPN, incluidos, entre otros, el tamaño del paquete, la mezcla de tráfico (TCP/UDP), las políticas de modelado o de limitación controlada en redes intermedias, el tiempo de Internet y los requisitos específicos de 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 las conexiones de Site-to-Site VPN de una gateway de tránsito, puede usar ECMP para conseguir un mayor ancho de banda de VPN agregando 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**
>
> Las VPN IPv6 admiten el mismo rendimiento (Gbps y PPS), MTU y límites de ruta que las VPN IPv4. No hay diferencias de rendimiento entre las conexiones IPv4 e IPv6 de VPN.

Unidad de transmisión máxima (MTU).

Site-to-Site VPN admite una unidad máxima de transmisión (MTU) de 1446 bytes y un tamaño máximo de segmento (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 de cliente de AWS Site-to-Site VPN.

No se admiten tramas gigantes. Para obtener más información, consulte Tramas gigantes en la Guía del usuario de Amazon EC2.

Las conexiones de Site-to-Site VPN no admiten la detección de MTU de la ruta.

Las limitaciones de MTU se aplican a las conexiones IPv4 e IPv6 de VPN.

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 revisión de la Guía del usuario de Site-to-Site VPN

En la siguiente tabla se describen las actualizaciones de la Guía del usuario de AWS Site-to-Site VPN.

Cambio	Descripción	Fecha
Compatibilidad de IPv6 con AWS Site-to-Site VPN para IP de túnel externo	VPN Site-to-Site admite ahora direcciones IPv6 para IP de túnel externo en conexiones de VPN de puerta de enlace de tránsito y WAN en la nube. Permite una migración completa a IPv6 con direccion es IPv6 tanto para las IP de túnel externo como para las IP de paquetes internos (IPv6 en IPv6), así como para las IP de túnel externo IPv6 con IP de paquetes internos IPv4 (IPv4 en IPv6).	1 de julio de 2025
Se ha actualizado la política administrada AWS AWSVPCS2SVpnServic eRolePolicy	Se han añadido nuevos permisos a la política administr ada de AWS que permiten a Site-to-Site VPN administr ar el secreto administrado de AWS Secrets Manager de la conexión de VPN.	27 de mayo de 2025
Se han actualizado las opciones de almacenam iento de claves compartidas previamente	Site-to-Site VPN es compatibl e ahora con AWS Secrets Manager para almacenar una clave compartida previamente.	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 agregado registros de ejemplo para conexiones de Site-to-Site VPN.	9 de diciembre de 2022
Utilidad de la configuración de descarga actualizada	Los clientes de Site-to-Site VPN pueden generar plantillas de configuración para dispositivos compatibles con Gateway de Cliente (CGW), lo que facilita la creación de conexiones VPN a AWS. Esta actualización agrega la compatibilidad con los parámetros de Intercambio de Clave de Internet versión 2 (IKEv2) para muchos dispositivos populares CGW e incluye dos nuevas API: GetVpnConnectionDeviceTypes y GetVpnConnectionDeviceSampleConfiguration.	21 de septiembre de 2021
Notificaciones de la conexión de VPN	Site-to-Site VPN envía automáticamente notificaciones sobre la conexión de VPN a AWS Health Dashboard.	29 de octubre de 2020
Iniciación de túnel de VPN	Puede configurar sus túneles de VPN de modo que AWS muestre los túneles.	27 de agosto de 2020

Modificar las opciones de conexión de VPN	Puede modificar las opciones de una conexión de 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
Compatibilidad con IPv	Los túneles VPN pueden admitir tráfico IPv6 dentro de los túneles.	12 de agosto de 2020
Combinar las guías de AWS Site-to-Site VPN	En esta versión, se combina el contenido de la Guía para administradores de red de AWS Site-to-Site VPN en esta guía.	31 de marzo de 2020
Conexiones de AWS Site-to-Site VPN aceleradas	Puede habilitar la aceleración para su conexión de AWS Site-to-Site VPN.	3 de diciembre de 2019
Modificar opciones de túnel de AWS Site-to-Site VPN	Puede modificar las opciones de un túnel de VPN en una conexión de AWS Site-to-Site VPN. También puede configurar opciones de túnel adicionales.	29 de agosto de 2019
AWS Private Certificate Authority Compatibilidad con certificados privados de	(Opcional) Certificado privado de AWS Private Certificate Authority para autenticar la VPN.	15 de agosto de 2019

Nueva guía del usuario de Site-to-Site VPN	En esta versión, el contenido de AWS Site-to-Site VPN (anteriormente conocido como VPN administrado por AWS) está separado de la Guía del usuario de Amazon VPC.	18 de diciembre de 2018
Modificar la gateway de destino	Puede modificar la gateway de destino de la conexión de AWS Site-to-Site VPN.	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 las métricas de CloudWatch de las conexiones de 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 de VPN de IPsec a Amazon VPC utilizando configuraciones de direccionamiento 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 rutas desde su VPN y enlaces de AWS Direct Connect a sus tablas de enrutamiento de VPC.	13 de septiembre de 2012

Site-to-Site VPN CloudHub y conexiones de 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