



Guía del usuario de

AWS Site-to-Site VPN



AWS Site-to-Site VPN: Guía del usuario de

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS Site-to-Site VPN?	1
Conceptos	1
Site-to-Site Características de la VPN	2
Site-to-Site Limitaciones de la VPN	3
Site-to-Site Recursos de VPN	3
Precios	4
Cómo funciona la Site-to-Site VPN	5
Gateway privada virtual	5
Puerta de enlace de tránsito	6
Dispositivo de gateway de cliente	7
Puerta de enlace de cliente	7
Puerta de enlace de cliente IPv6	8
Conexiones de VPN IPv6	8
Opciones de túnel de VPN	9
Opciones de ancho de banda del túnel	10
Túneles de gran ancho de banda	11
Configure las opciones de túnel	13
Opciones de autenticación de túneles de VPN	21
Claves previamente compartidas	21
Certificado privado de AWS Private Certificate Authority	21
Opciones de iniciación de túnel de VPN	22
Opciones de iniciación de IKE de túnel de VPN	22
Reglas y limitaciones	23
Uso de opciones de iniciación de túnel de VPN	23
Sustitución de los puntos de enlace	24
Sustituciones de puntos de conexión iniciadas por el cliente	24
Sustituciones de puntos de conexión administrados por AWS	25
Ciclo de vida del punto de conexión del túnel	25
Opciones de gateway de cliente	31
Opciones de puerta de enlace de cliente IPv6	35
Conexiones de VPN aceleradas	35
Habilitación de la aceleración	35
Reglas y restricciones	36
Site-to-Site opciones de enrutamiento de VPN	37

Direccionamiento estático y dinámico	37
Tablas de enrutamiento y prioridad de rutas	38
Enrutamiento durante las actualizaciones de punto de enlace del túnel de VPN	41
Tráfico IPv4 e IPv6	42
Concentradores VPN	43
Características y servicios de puerta de enlace compatibles	43
Ancho de banda	44
Enrutamiento	44
Asignación de direcciones IP	45
Supervisión	45
Mantenimiento de túneles	45
Precios	45
Comience con la Site-to-Site VPN	46
Requisitos previos	46
Creación de una gateway de cliente	48
Crear una gateway de destino	49
Creación de una gateway privada virtual	49
Crear una puerta de enlace de tránsito	50
Configuración del enrutamiento	51
(Gateway privada virtual) Habilitar la propagación de rutas en la tabla de enrutamiento	51
(Gateway de tránsito) Agregar una ruta a la tabla de enrutamiento	52
Actualización de su grupo de seguridad	53
Para crear una conexión de VPN	53
Para descargar el archivo de configuración	56
Configurar el dispositivo de gateway de cliente	57
Site-to-Site Escenarios arquitectónicos de VPN	58
Conexiones de VPN únicas y múltiples	59
Conexión Site-to-Site VPN única	59
Conexión Site-to-Site VPN única con una puerta de enlace de tránsito	60
Múltiples conexiones Site-to-Site VPN	60
Varias conexiones Site-to-Site VPN con una puerta de enlace de tránsito	61
Site-to-Site Conexión VPN con Direct Connect	62
Conexión Site-to-Site VPN IP privada con Direct Connect	63
Comunicaciones seguras entre conexiones VPN mediante VPN CloudHub	64
Descripción general de	64
Precios	65

Conexiones de VPN redundantes	66
Site-to-Site dispositivos VPN de puerta de enlace para clientes	69
Requisitos	70
Prácticas recomendadas	73
Reglas de firewall	76
Archivos de configuración de enrutamiento estático y dinámico	78
Archivos de configuración de enrutamiento estático descargables	80
Archivos de configuración dinámica descargables	94
Configuración de Windows Server como dispositivo de puerta de enlace de cliente	107
Configuración de instancias de Windows	107
Paso 1: Crear una conexión de VPN y configurar la VPC	108
Paso 2: Descargar el archivo de configuración de la conexión de VPN	109
Paso 3: Configuración de Windows Server	112
Paso 4: Configurar el túnel de VPN	113
Paso 5: Habilitar la detección de gateways inactivas	120
Paso 6: Comprobar la conexión de VPN	121
Solución de problemas de dispositivos de puerta de enlace de cliente	122
Dispositivo con BGP	123
Dispositivo sin BGP	126
Cisco ASA	129
Cisco IOS	134
Cisco IOS sin BGP	140
Juniper JunOS	146
Juniper ScreenOS	151
Yamaha	154
Integración de eero	159
Trabaja con una Site-to-Site VPN	161
Cree y administre concentradores VPN	161
Cree un concentrador de VPN	162
Administre las etiquetas de VPN Concentrator	164
Eliminar un concentrador de VPN	168
Para crear una conexión de VPN	170
Cree una conexión VPN mediante la consola	170
Cree una conexión de puerta de enlace de tránsito VPN mediante la CLI o la API	173
Cree una conexión VPN Cloud WAN mediante la CLI o la API	176
Cree una conexión de concentrador VPN mediante la CLI o la API	179

Ver las conexiones VPN	181
Prueba de una conexión de VPN	184
Eliminación de una conexión de VPN y una puerta de enlace	186
Eliminación de una conexión de VPN	187
Eliminación de una puerta de enlace de cliente	187
Desasociación y eliminación de una puerta de enlace privada virtual	188
Modificación de la puerta de enlace de destino de una conexión de VPN	189
Paso 1: Crear la puerta de enlace de destino nueva	190
Paso 2: Actualizar las rutas estáticas (condicional)	190
Paso 3: Migrar a una nueva gateway	191
Paso 4: Actualizar tablas de enrutamiento de VPC	191
Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino (condicional)	193
Paso 6: Actualizar el ASN de la puerta de enlace de cliente (condicional)	193
Modificar las opciones de conexión de VPN	193
Modifique el ancho de banda del	194
Modificación de las opciones del túnel de VPN	196
Edición de estáticas en una conexión de VPN	197
Cambio de la puerta de enlace de cliente para una conexión de VPN	198
Remplazo de credenciales comprometidas	198
Rotación de certificados de punto de conexión de túnel de VPN	199
VPN de IP privada con Direct Connect	200
Beneficios de la VPN de IP privada	200
Cómo funciona la VPN de IP privada	201
Requisitos previos	201
Creación de una VPN de IP privada a través de Direct Connect	203
Seguridad	209
Características de seguridad mejoradas con Secrets Manager	210
Cambio de la clave compartida previamente de Secrets Manager	210
Cambio del modo de almacenamiento de claves compartidas previamente	211
Protección de datos	212
Privacidad del tráfico entre redes	213
Identity and Access Management	214
Público	215
Autenticación con identidades	215
Administración del acceso con políticas	217
Cómo AWS Site-to-Site La VPN funciona con IAM	218

Identity-based ejemplos de políticas	224
Resolución de problemas	227
AWS políticas gestionadas	230
Cómo utilizar roles vinculados a servicios	231
Resiliencia	233
Dos túneles por conexión de VPN	233
Redundancia	234
Seguridad de la infraestructura	234
Supervise una conexión Site-to-Site VPN	235
Herramientas de supervisión	236
Herramientas de supervisión automatizadas	236
Herramientas de supervisión manuales	236
Site-to-Site registros de VPN	237
Ventajas de los registros de Site-to-Site VPN	238
Restricciones de tamaño de la política de recursos de Amazon CloudWatch Logs	239
Site-to-Site Contenido del registro de la VPN	239
Ejemplo de formato de registro para los registros BGP de Tunnel	250
Requisitos de IAM para publicar en los registros CloudWatch	250
Vea la configuración de los registros de la Site-to-Site VPN	252
Habilite los registros de Site-to-Site VPN	252
Deshabilite los registros de Site-to-Site VPN	254
Supervise los túneles Site-to-Site VPN mediante CloudWatch	256
Dimensiones y métricas de VPN	256
Ver las CloudWatch métricas de VPN	258
Cree CloudWatch alarmas para monitorear los túneles de VPN	259
AWS Health y eventos de Site-to-Site VPN	262
Notificaciones de sustitución de puntos de enlace de un túnel	262
Notificaciones de VPN con un solo túnel	262
Cuotas	263
Site-to-Site Recursos de VPN	263
Rutas	264
Ancho de banda y rendimiento	265
Unidad de transmisión máxima (MTU).	266
Recursos de cuotas adicionales	267
Historial de revisión	268
.....	cclxxiv

¿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 sus dispositivos remotos desde su VPC creando una conexión AWS Site-to-Site VPN(Site-to-Site VPN) y configurando el enrutamiento para que pase el tráfico a través de la conexión.

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

Contenido

- [Conceptos](#)
- [Site-to-Site Características de la VPN](#)
- [Site-to-Site Limitaciones de la VPN](#)
- [Site-to-Site Recursos de VPN](#)
- [Precios](#)

Conceptos

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

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

Cada conexión de VPN incluye dos túneles de VPN que puede utilizar simultáneamente para conseguir alta disponibilidad.

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

- Puerta de enlace privada virtual: una puerta de enlace privada virtual es el punto final de la conexión VPN en el lado Amazon de la conexión Site-to-Site VPN que se puede conectar a una sola VPC.
- Puerta de enlace de tránsito: un centro de tránsito que se puede usar para interconectar redes múltiples VPCs y locales, y como punto final de VPN para el lado Amazon de la conexión Site-to-Site VPN.
- Túnel de gran ancho de banda: configuración de túnel que admite un ancho de banda de hasta 5 Gbps por túnel, en comparación con el estándar de 1,25 Gbps. Disponible para conexiones VPN conectadas a Transit Gateway o Cloud WAN.

Site-to-Site Características de la VPN

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

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

- IPv6 IP de túnel exterior con IP de paquete IPv6 interior (IPv6-in-IPv6)
- IPv6 IP de túnel exterior con IP de paquete IPv4 interior (IPv4-in-IPv6)

Site-to-Site Limitaciones de la VPN

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

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

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

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

Site-to-Site Recursos de VPN

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

- Consola de administración de AWS— Proporciona una interfaz web que puede utilizar para acceder a sus recursos de Site-to-Site VPN.
- AWS Command Line Interface(AWS CLI) — Proporciona comandos para un amplio conjunto de AWS servicios, incluido Amazon VPC, y es compatible con Windows, macOS y Linux. Las líneas de comandos se incluyen en la AWS Site-to-Site VPN referencia de línea de comandos más amplia EC2
- Para obtener información general acerca de estas interfaces de líneas de comandos, consulte [AWS Command Line Interface](#).

- Para ver la lista de EC2 comandos disponibles, incluidos los comandos de Site-to-Site VPN, consulte la Referencia de la [EC2 línea](#) de comandos.

 Note

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

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

Precios

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

Se le cobrará por la transferencia de datos de Amazon EC2 a Internet. Para obtener más información, consulta [Data Transfer](#) en la página de precios de Amazon EC2 On-Demand.

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

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

Cómo AWS Site-to-Site VPN funciona

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

- Una [puerta de enlace privada virtual](#) o una [puerta de enlace de tránsito](#)
- Un [dispositivo de puerta de enlace de cliente](#)
- Una [puerta de enlace de cliente](#)

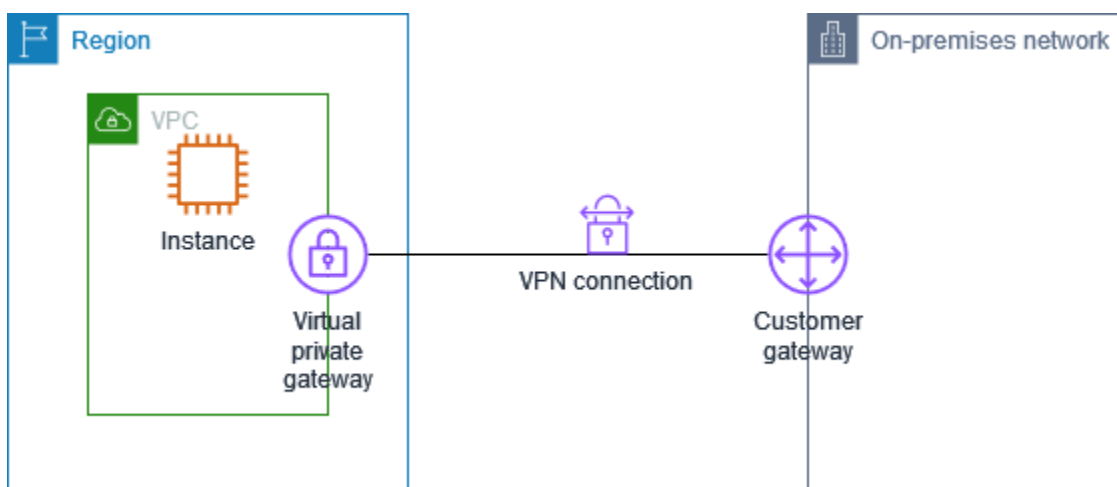
La conexión VPN ofrece dos túneles VPN entre una puerta de enlace privada virtual o una puerta de enlace de tránsito, por un AWS lado, y una puerta de enlace de cliente, por el lado local.

Para obtener más información sobre las cuotas de Site-to-Site VPN, consulte [AWS Site-to-Site VPN cuotas](#).

Gateway privada virtual

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

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



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

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

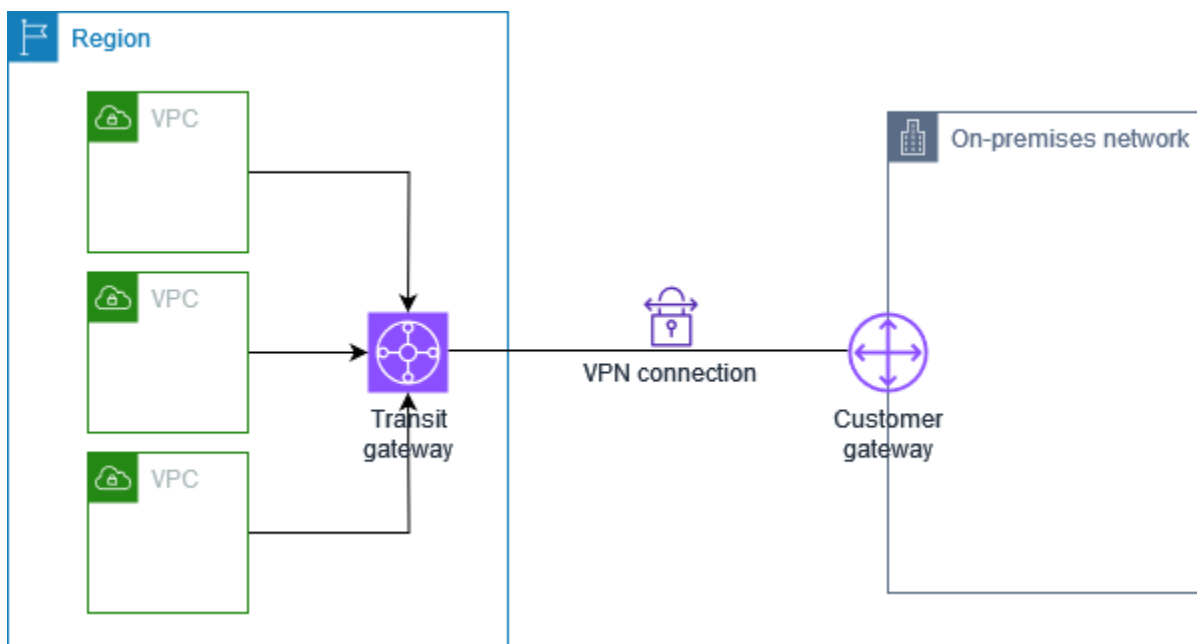
Note

Las puertas de enlace privadas virtuales no admiten IPv6 para Site-to-Site las conexiones 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 Site-to-Site VPN como un archivo adjunto en una puerta de enlace 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.



Tu conexión Site-to-Site VPN en una pasarela de tránsito puede admitir el tráfico de IPv4 o IPv6 dentro de los túneles de la 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 puerta de enlace de destino de una conexión Site-to-Site VPN de una puerta de enlace privada virtual a una puerta de enlace de tránsito. Para obtener más información, consulte [the section called “Modificación de la puerta de enlace de destino de una conexión de VPN”](#).

Dispositivo de gateway de cliente

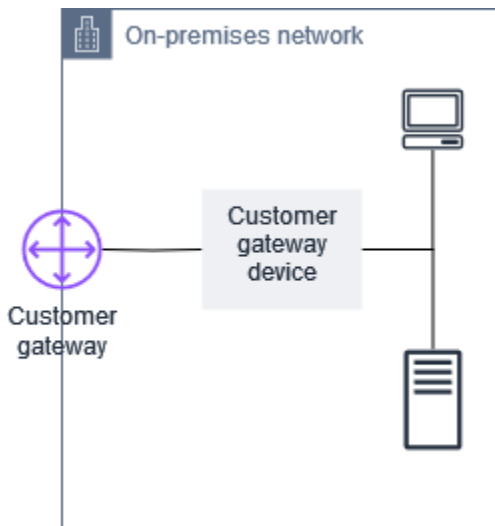
Un dispositivo de puerta de enlace para clientes es un dispositivo físico o una aplicación de software que se encuentra en su lado de la conexión Site-to-Site VPN. Usted configura el dispositivo para que funcione con la conexión Site-to-Site VPN. Para obtener más información, consulte [AWS Site-to-Site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

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

Si utiliza 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. Al crear una pasarela de clientes, proporciona información sobre su dispositivo a AWS. Para obtener más información, consulte [the section called “Opciones de gateway de cliente”](#).



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

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 AWS de administración 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

Site-to-Site Las conexiones VPN 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 exterior IPv4 con paquetes internos de IPv6: permite que IPv6 applications/transport entre en el túnel 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-001122334455aabbcc --options
OutsideIPAddressType=Ipv6,TunnelInsideIpVersion=ipv6,TunnelOptions=[{StartupAction=start},
{StartupAction=start}]
```

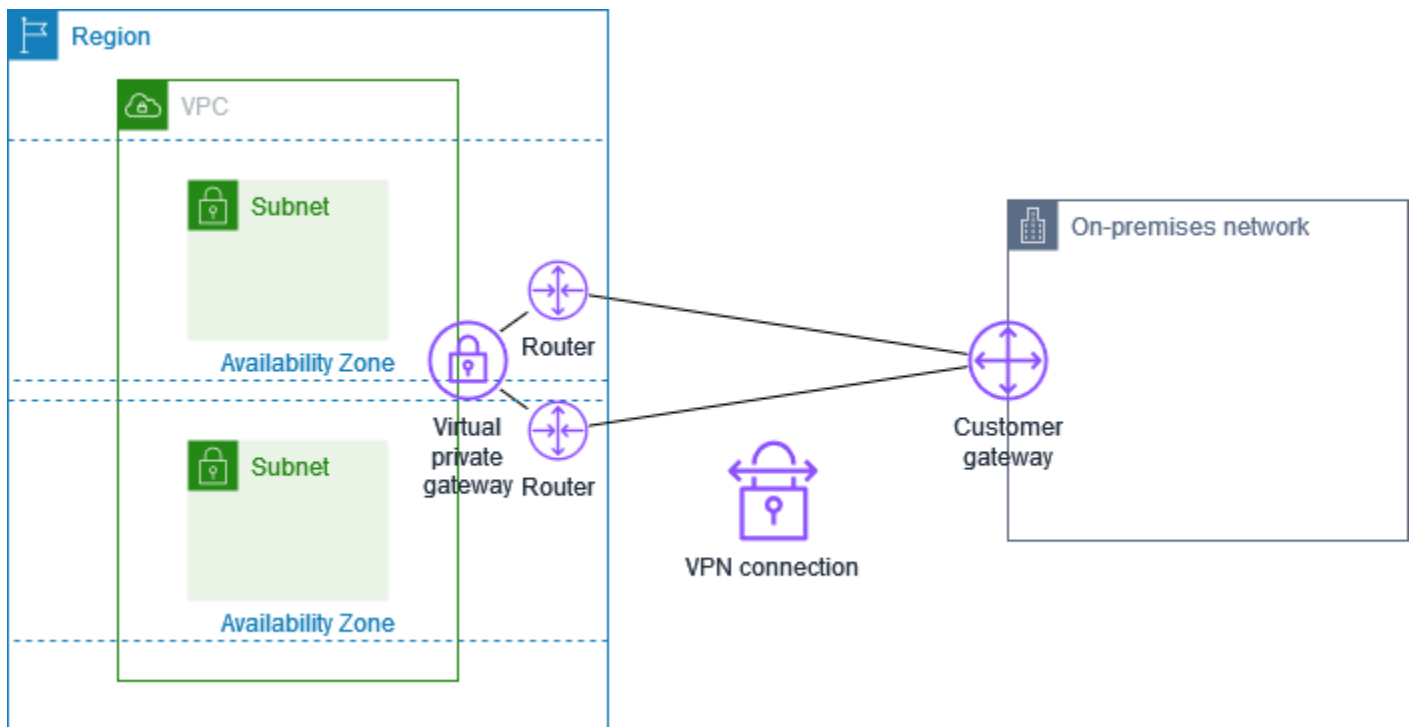
Puede ver las direcciones IPv6 asignadas a su conexión de VPN mediante el comando `describe-vpn-connection` de la CLI.

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

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

El siguiente diagrama muestra los dos túneles de la conexión de VPN. Cada túnel termina en una zona de disponibilidad diferente para aumentar la disponibilidad. El tráfico desde la red local AWS

utiliza ambos túneles. El tráfico que se dirige AWS a la red local prefiere uno de los túneles, pero puede conmutar automáticamente por error al otro túnel si se produce un fallo lateral. AWS



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

Opciones de ancho de banda del túnel

Puede configurar la capacidad de ancho de banda de sus túneles VPN:

- Ancho de banda estándar: hasta 1,25 Gbps por túnel (predeterminado)
- Túnel de gran ancho de banda (LBT): hasta 5 Gbps por túnel

Los túneles de gran ancho de banda están disponibles solo para las conexiones VPN conectadas a Transit Gateway o Cloud WAN. Para obtener más información, consulte [Túneles de gran ancho de banda](#).

Note

Site-to-Site Los puntos finales de los túneles VPN evalúan las propuestas de su pasarela de clientes empezando por el valor configurado más bajo de la lista que aparece a continuación, independientemente del pedido de propuestas de la pasarela de clientes. Puede usar el `modify-vpn-connection-options` comando para restringir la lista de opciones que aceptarán AWS los puntos finales. Para obtener más información, consulte las [opciones de modify-vpn-connection](#) en la Referencia de la línea de comandos de Amazon EC2.

Túneles de gran ancho de banda

Los túneles de gran ancho de banda permiten configurar túneles Site-to-Site VPN que admiten un ancho de banda de hasta 5 Gbps por túnel, en comparación con el estándar de 1,25 Gbps. Hay túneles de gran ancho de banda disponibles para las conexiones VPN conectadas a Transit Gateway o Cloud WAN. Esto elimina o reduce la necesidad de implementar protocolos complejos como el ECMP (ruta múltiple de igual costo) para lograr un mayor ancho de banda y garantiza un ancho de banda de túnel constante de 5 Gbps por túnel. Los túneles de gran ancho de banda están diseñados para usarse en los siguientes casos de uso:

- Conectividad de centros de datos: Support aplicaciones híbridas con uso intensivo de ancho de banda, migraciones de macrodatos o arquitecturas de recuperación ante desastres que requieren una conectividad de alta capacidad entre las cargas de trabajo de AWS y los centros de datos locales.
- Respaldo de Direct Connect: proporcione conectividad de respaldo o superpuesta para circuitos Direct Connect de alta capacidad (más de 10 Gbps+) a centros de datos locales o instalaciones de colocación.

Disponibilidad por región

Los túneles de gran ancho de banda están disponibles en todas las regiones, excepto en las siguientes:

No disponible Regiones de AWS

AWS Región	Description (Descripción)
ap-southeast-4	Asia-Pacífico (Melbourne)

AWS Región	Description (Descripción)
ca-west-1	Oeste de Canadá (Calgary)
eu-central-2	Europa (Zúrich)
il-central-1	Israel (Tel Aviv)
me-central-1	Medio Oriente (EAU)

Requisitos y limitaciones

- Disponible solo para las conexiones VPN conectadas a una puerta de enlace de tránsito o a Cloud WAN. No es compatible con los archivos adjuntos de una puerta de enlace privada virtual.
- Los dos túneles de una conexión VPN deben usar la misma configuración de ancho de banda (1,25 Gbps o 5 Gbps).
- No se admite la VPN acelerada.
- Todas las demás funciones principales de la VPN, como la VPN con IP privada, el enrutamiento y el mantenimiento de túneles, funcionan de la misma manera con Large Bandwidth Tunnel.
- El límite de MTU sigue siendo de 1500 bytes. [Obtenga más información](#) sobre cómo ajustar los tamaños de MTU y MSS de acuerdo con los algoritmos utilizados.
- Puede modificar el ancho de banda del túnel de las conexiones VPN existentes. Para obtener más información, consulte [Modifique el ancho de banda del](#).
- Las pasarelas de cliente (CGW) solo con una IP fija se pueden utilizar con túneles de gran ancho de banda.
- Las pasarelas de cliente (CGW) sin una dirección IP no se pueden utilizar con túneles de gran ancho de banda.
- Los túneles de gran ancho de banda no admiten cambios en el NAT-T puerto mientras el túnel está establecido.
- Los paquetes que requieren fragmentación pueden experimentar un rendimiento inferior. [Obtenga más información](#).

Precios de túneles de gran ancho de banda

Puede encontrar información sobre los precios de las conexiones VPN de gran ancho de banda en la página de [precios de las AWS VPN](#).

Escalar más allá de los 5 Gbps

Para requisitos de ancho de banda que superen los 5 Gbps por túnel, puede utilizar el ECMP en varias conexiones VPN. Por ejemplo, puede lograr un ancho de banda de 20 Gbps si implementa dos conexiones VPN con túneles de gran ancho de banda y utiliza el ECMP en los cuatro túneles.

Configure las opciones de túnel para AWS Site-to-Site VPN

Esta sección proporciona una guía completa sobre la configuración de las opciones de túnel para AWS Site-to-Site VPN las conexiones y abarca parámetros esenciales como la detección de puntos muertos, las versiones de IKE y la configuración de cifrado. Puede personalizar estas opciones de túnel para optimizar la seguridad, el rendimiento y la compatibilidad de su conexión VPN con la infraestructura de red local.

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

Note

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

Tiempo de espera de detección de pares muertos (DPD)

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

Predeterminado: 40

Acción de tiempo de espera de DPD

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

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

Para obtener más información, consulte [AWS Site-to-Site VPN opciones de inicio de túnel](#).

Valor predeterminado: **Clear**

Opciones de registro de VPN

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

Para obtener más información, consulte [AWS Site-to-Site VPN registros](#).

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

Versiones de IKE

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

Valores predeterminados: **ikev1**, **ikev2**

Túnel interior de CIDR IPv4

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

Note

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

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

- 169.254.0.0/30
- 169.254.1.0/30
- 169.254.2.0/30
- 169.254.3.0/30
- 169.254.4.0/30
- 169.254.5.0/30
- 169.254.169.252/30

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

Pre-shared almacenamiento de claves

Tipo de almacenamiento de la clave compartida previamente:

- Estándar: la clave previamente compartida se almacena directamente en el servicio Site-to-Site VPN.
- Secrets Manager: la clave previamente compartida se almacena mediante AWS Secrets Manager. Para obtener más información acerca de Secrets Manager, consulte [Características de seguridad mejoradas con Secrets Manager](#).

Ancho de banda del túnel

El ancho de banda compatible con el túnel.

- Estándar: el ancho de banda del túnel está establecido en un máximo de 1,25 Gbps por túnel (predeterminado).
- Grande: el ancho de banda del túnel alcanza un máximo de 5 Gbps por túnel.

Note

El tamaño grande solo está disponible para las conexiones VPN conectadas a una pasarela de tránsito o a una WAN de nube. No es compatible con las conexiones de pasarelas de enlace privadas virtuales.

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 CIDR debe ser único en todas las conexiones Site-to-Site VPN que utilizan la misma puerta de

enlace 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 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 rango se usa para proponer rutas, pero no impone restricciones de tráfico, ya que AWS utiliza exclusivamente VPN basadas en rutas. Policy-based No se admiten las VPN porque AWS limitarían la capacidad 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.

Predeterminado: 0.0.0. 0/0

CIDR de red IPv4 remota

(Solo para conexión VPN IPv4) El rango CIDR utilizado durante la negociación de la fase 2 de IKE para el AWS lado del túnel 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 las VPN basadas en políticas porque carecen de la flexibilidad necesaria para escenarios de enrutamiento complejos y son incompatibles con funciones como las pasarelas de tránsito y VPN Equal Cost Multi-Path (ECMP). 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.

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 para conexión VPN IPv6) El rango CIDR de IPv6 está en el AWS lado que puede comunicarse a través de los túneles VPN.

Predeterminado:: :/0

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

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 de la fase 2 Diffie-Hellman (DH)

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.

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

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

Predeterminado: 28 800 (8 horas)

Vida útil de la fase 2

Note

AWS inicie los cambios de clave con los valores de temporización establecidos en los campos Duración de la fase 1 y Duración de la fase 2. Si tales campos de vida útil son

diferentes a los valores de protocolo de enlace negociados, esto puede interrumpir la conectividad del túnel.

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

Predeterminado: 3600 (1 hora)

Pre-shared clave (PSK)

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

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

Predeterminado: una cadena alfanumérica de 32 caracteres.

Difusión de cambio de clave

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

Puede especificar un valor porcentual entre 0 y 100.

Predeterminado: 100

Tiempo de margen de cambio de clave

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

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

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

Predeterminado: 270 (4,5 minutos)

Tamaño de paquetes del período de reproducción

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

Puede especificar un valor comprendido entre 64 y 2048.

Predeterminado: 1024

Acción de inicio

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

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

Para obtener más información, consulte [AWS Site-to-Site VPN opciones de inicio de túnel](#).

Valor predeterminado: Add

Control del ciclo de vida del punto de conexión del túnel

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

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

Valor predeterminado: Off

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

- [Paso 5: Crear una conexión de VPN](#)
- [Modificar opciones de túnel de AWS Site-to-Site VPN](#)

AWS Site-to-Site VPN Opciones 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 [Site-to-Site dispositivos VPN de puerta de enlace para clientes](#).
- 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 “Service-linked funciones”](#).

 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 VPN opciones de inicio de túnel

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

Opciones de iniciación de IKE de túnel de VPN

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

- **Acción de inicio:** acción que se debe realizar al establecer el túnel de VPN para una conexión de VPN nueva o modificada. De forma predeterminada, el dispositivo de gateway de cliente inicia el proceso de negociación de IKE para mostrar el túnel. Puede AWS especificar que, en su lugar, se inicie el proceso de negociación de IKE.
- **Acción de tiempo de espera de DPD:** la acción que se debe realizar después de que se cumpla el tiempo de espera de detección de pares muertos (DPD). De forma predeterminada, la sesión de IKE se detiene, el túnel se desactiva y se eliminan las rutas. Puede especificar que AWS debe

reiniciarse la sesión de IKE cuando se agote el tiempo de espera de DPD, o puede especificar que no se AWS debe realizar ninguna acción cuando se agote el tiempo de espera de DPD.

Reglas y limitaciones

Se aplican las siguientes reglas y limitaciones:

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

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

Uso de opciones de iniciación de túnel de VPN

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

- Para crear una nueva conexión de VPN y especificar las opciones de iniciación del túnel de VPN: [Paso 5: Crear una conexión de VPN](#)

- Para modificar las opciones de iniciación del túnel de VPN en una conexión de VPN existente:
[Modificar opciones de túnel de AWS Site-to-Site VPN](#)

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

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

Temas

- [Sustituciones de puntos de conexión iniciadas por el cliente](#)
- [Sustituciones de puntos de conexión administrados por AWS](#)
- [AWS Site-to-Site VPN control del ciclo de vida de los puntos finales](#)

Sustituciones de puntos de conexión iniciadas por el cliente

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

Modificación	Acción de la API	Impacto en el túnel
Modificación de la gateway de destino de la conexión de VPN	ModifyVpnConnection	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Cambio de la gateway de cliente de la conexión de VPN	ModifyVpnConnection	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.
Modificación de las opciones de la conexión de VPN	ModifyVpnConnectionOptions	Los dos túneles dejan de estar disponibles mientras se aprovisionan los nuevos puntos de enlace del túnel.

Modificación	Acción de la API	Impacto en el 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 gestionado y actualiza periódicamente los puntos finales de los túneles de la VPN. Estas actualizaciones se producen por una variedad de razones, entre las que se incluyen las siguientes:

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

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

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

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

Note

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

Temas

- [Cómo funciona el control del ciclo de vida del punto de conexión del túnel](#)
- [Active el control AWS Site-to-Site VPN del ciclo de vida de los puntos finales](#)
- [Compruebe si el control del ciclo de vida de los puntos finales del AWS Site-to-Site VPN túnel está activado](#)
- [Compruebe si hay actualizaciones de AWS Site-to-Site VPN túnel disponibles](#)
- [Acepte una actualización de mantenimiento AWS Site-to-Site VPN del túnel](#)
- [Desactive el control del ciclo de vida de los terminales del AWS Site-to-Site VPN túnel](#)

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

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

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

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

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

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

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

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

 Note

De forma predeterminada, al activar la característica para una conexión VPN existente, se iniciará la sustitución del punto de conexión del túnel al mismo tiempo. Si desea activar la característica, pero no iniciar inmediatamente la sustitución del punto de conexión del túnel, puede utilizar la opción omitir la sustitución del túnel.

Existing VPN connection

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

Para habilitar el control del ciclo de vida de los puntos finales del túnel mediante 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 de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Modificar opciones de túnel de VPN.
5. Seleccione el túnel específico que desea modificar; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. En Control del ciclo de vida del punto de conexión del túnel, seleccione la casilla Habilitar.
7. (Opcional) Seleccione Omitir la sustitución del túnel.
8. Seleccione Save changes (Guardar cambios).

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

Usa el [modify-vpn-tunnel-options](#) comando para activar el control del ciclo de vida de los puntos finales del túnel.

New VPN connection

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

Para habilitar el control del ciclo de vida de los puntos finales del túnel durante la creación de una nueva conexión VPN mediante 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.
3. Elija Create VPN Connection (Crear conexión VPN).
4. En las secciones de opciones del Túnel 1 y opciones del Túnel 2, en Control del ciclo de vida del punto de conexión del túnel, seleccione Habilitar.
5. Elija Create VPN Connection (Crear conexión de VPN).

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

Usa el [create-vpn-connection](#) comando para activar el control del ciclo de vida de los puntos finales del túnel.

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

Puede comprobar si el control del ciclo de vida de los puntos finales del túnel está habilitado en un túnel VPN existente mediante la CLI 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 [Habilitación del control del ciclo de vida del punto de conexión del túnel de](#) .
- Si el control del ciclo de vida de los puntos de conexión del túnel está habilitado y desea desactivarlo, consulte [Desactivación del control del ciclo de vida del punto de conexión del túnel de](#) .

Para comprobar si el control del ciclo de vida de los puntos finales del túnel está habilitado, utilice 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 de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Seleccione la pestaña Detalles del túnel.

5. En los detalles del túnel, busque Control del ciclo de vida del punto de conexión del túnel, que indicará si la característica está Habilitada o Desactivada.

Para comprobar si el control del ciclo de vida de los puntos finales del túnel está activado, utilice el AWS CLI

Utilice el [describe-vpn-connections](#) comando para comprobar si el control del ciclo de vida de los puntos finales del túnel está activado.

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

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

Para comprobar si hay actualizaciones disponibles, utilice la 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 de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Seleccione la pestaña Detalles del túnel.
5. Compruebe la columna Mantenimiento pendiente. El estado será Disponible o Ninguno.

Para comprobar si hay actualizaciones disponibles, utilice el AWS CLI

Utilice el comando [get-vpn-tunnel-replacement-status](#) para comprobar si hay actualizaciones disponibles.

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

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

 Note

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

Para aceptar una actualización de mantenimiento disponible mediante el 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 de la izquierda, selecciona Conexiones Site-to-Site VPN.
3. Seleccione la conexión adecuada en Conexiones de VPN.
4. Elija Acciones y, a continuación, Sustituir túnel de VPN.
5. Seleccione el túnel específico que desea sustituir; para ello, elija la dirección IP fuera del túnel de VPN adecuada.
6. Elija Reemplazar.

Para aceptar una actualización de mantenimiento disponible mediante el AWS CLI

Utilice el [replace-vpn-tunnel](#) comando para aceptar una actualización de mantenimiento disponible.

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

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

 Note

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

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

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

Utilice el [modify-vpn-tunnel-options](#) comando para desactivar el control del ciclo de vida de los puntos finales 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

Elemento	Descripción
	• 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 VPN opciones de enrutamiento.

Elemento	Descripción
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 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 certificado 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 subordinada de 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 Certificate Authority y luego especifica el certificado al configurar la gateway de cliente. Para obtener información sobre la creación de un certificado privado, consulte la sección de creación y administración de una CA privada en la Guía del usuario de AWS Private 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
```

AWS Site-to-Site VPN Conexiones aceleradas

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

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

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

Habilitación de la aceleración

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

pasarela de tránsito. Para obtener más información y ver los pasos, consulte [Crear una AWS Site-to-Site VPN conexión](#).

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

Reglas y restricciones

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

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

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

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

Para obtener más información sobre la prioridad de una ruta, consulte [Tablas de enrutamiento y prioridad de rutas](#).

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

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

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

Temas

- [Enrutamiento estático y dinámico en AWS Site-to-Site VPN](#)
- [Tablas de enrutamiento y prioridad de AWS Site-to-Site VPN enrutamiento](#)
- [Enrutamiento durante las actualizaciones de punto de enlace del túnel de VPN](#)
- [Tráfico de IPv4 e IPv6 en AWS Site-to-Site VPN](#)

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

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

 Note

Site-to-Site Los concentradores VPN solo admiten el enrutamiento BGP. El enrutamiento estático no es compatible con las conexiones VPN que utilizan un concentrador Site-to-Site VPN.

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

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

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

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

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

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

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

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

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

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

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

- Rutas propagadas por BGP desde una conexión Direct Connect

Las rutas de Blackhole no se propagan a la pasarela de un cliente de Site-to-Site VPN a través de BGP.

- Rutas estáticas añadidas manualmente para una conexión VPN Site-to-Site
- Rutas propagadas por BGP desde una conexión VPN Site-to-Site
- Para los prefijos coincidentes en los que cada conexión Site-to-Site VPN usa BGP, se compara la RUTA AS y se prefiere el prefijo con la RUTA AS más corta.

 Note

AWS recomienda encarecidamente utilizar dispositivos de puerta de enlace para clientes que admitan el enrutamiento asimétrico.

Para los dispositivos de puerta de enlace de clientes que admiten enrutamiento asimétrico, no recomendamos 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 los AS PATHs tienen la misma longitud y si el primer AS de la AS_SEQUENCE es el mismo en varias rutas, se comparan multi-exit discriminators (MEDs). Se prefiere la ruta con el valor de MED más bajo.

La prioridad de ruta se ve afectada durante las [actualizaciones del punto de enlace del túnel de la VPN](#).

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

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

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

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

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

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

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

Note

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

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.

AWS Site-to-Site VPN Concentradores

AWS Site-to-Site VPN Concentrator es una nueva característica que simplifica la conectividad multisitio para empresas distribuidas. VPN Concentrator es adecuado para clientes que necesitan conectar más de 25 sitios remotos a AWS, y cada sitio necesita poco ancho de banda (menos de 100 Mbps).

Características y servicios de puerta de enlace compatibles

Los concentradores VPN solo son compatibles con Transit Gateway. Esta función no es compatible con Cloud WAN ni con Virtual Private Gateway.

En la siguiente tabla se describen las funciones compatibles con Site-to-Site VPN Concentrator:

Característica	¿Se admite?
IPv6	Sí
Conexiones VPN privadas de Direct Connect	No
VPN acelerada	Sí

Característica	¿Se admite?
Varios dispositivos de puerta de enlace para clientes desde el mismo sitio	Sí. Sin embargo, cada dispositivo de puerta de enlace del cliente debe tener una dirección IP única.
Restricciones geográficas	No. Puede adjuntar un sitio ubicado en cualquier región a un concentrador en cualquier AWS región.
Site-to-Site Registros de VPN	Sí. Puede generar registros de VPN para todos los sitios conectados al Concentrador o de forma individual.
Soporte de cifrado de Transit Gateway	No

Ancho de banda

Actualmente, los concentradores Site-to-Site VPN admiten un ancho de banda total de 5 Gbps. Cada sitio puede admitir un ancho de banda máximo de 100 Mbps. Sin embargo, si necesita un ancho de banda superior, póngase en contacto con AWS Support.

Enrutamiento

Site-to-Site Los concentradores VPN solo admiten el enrutamiento BGP (Border Gateway Protocol). No se admite el enrutamiento estático.

Todas las puertas de enlace de los clientes conectadas a Site-to-Site VPN Concentrador utilizan el mismo conector de Site-to-Site VPN Concentrador a la puerta de enlace de tránsito para el enrutamiento. Cada sitio que se conecte al concentrador Site-to-Site VPN puede enviar un máximo de 5000 rutas desde la pasarela de tránsito a la pasarela del cliente y 1000 rutas desde la pasarela del cliente a la pasarela de tránsito.

Asignación de direcciones IP

Cada conexión VPN a través del concentrador de Site-to-Site VPN seguirá teniendo una dirección IP de AWS única (una por túnel).

Supervisión

Las conexiones Site-to-Site VPN a través de concentradores VPN admiten las mismas métricas que las conexiones VPN normales.

Si habilitas los registros de flujo de Transit Gateway en el dispositivo adjunto al concentrador VPN, verás los registros de flujo de todo el tráfico que entra y sale de todos los sitios remotos conectados al concentrador.

Mantenimiento de túneles

El mantenimiento del túnel funciona de la misma manera que los túneles Site-to-Site VPN estándar existentes para ambos puntos finales cuando se utiliza un concentrador de Site-to-Site VPN. Para obtener más información, consulte [Sustitución de los puntos de enlace](#).

Precios

Puede encontrar información sobre los precios de Site-to-Site VPN Concentrator en la página de [precios de VPN de AWS](#).

Comience con AWS Site-to-Site VPN

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

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

Tareas

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

Tareas relacionadas

- Para crear una conexión VPN para AWS Cloud WAN, consulta [Cree una conexión VPN Cloud WAN mediante la CLI o la API](#).
- Para crear una conexión de VPN en una puerta de enlace de tránsito, consulte [Para crear una conexión de VPN](#).

Requisitos previos

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

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

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

Paso 1: Crear una puerta de enlace de cliente

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

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

Note

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

Para crear una gateway de cliente con la consola

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

- IPv6- Especifique una IPv6 dirección para su dispositivo de pasarela de clientes. Esta opción es necesaria al crear una conexión VPN con el túnel IPv6 exterior IPs.
7. En 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 consultas de Amazon EC2)
- [create-customer-gateway](#) (AWS CLI)

Ejemplo de creación de una pasarela de IPv6 clientes:

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

- [New-EC2CustomerGateway](#) (AWS Tools for Windows PowerShell)

Paso 2: Crear una puerta de enlace de destino

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

Creación de una gateway privada virtual

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

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

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

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

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

- [CreateVpnGateway](#) (API de consultas 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 consultas de Amazon EC2)
- [attach-vpn-gateway](#) (AWS CLI)
- [Add-EC2VpnGateway](#) (AWS Tools for Windows PowerShell)

Crear una puerta de enlace de tránsito

Para obtener más información acerca de cómo crear una gateway de tránsito, consulte [Gateways de tránsito](#) en Gateways de tránsito de Amazon VPC.

Paso 3: Configuración del enrutamiento

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

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

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

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

Note

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

Para habilitar la propagación de rutas utilizando la consola

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

Note

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

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

Para deshabilitar la propagación de rutas utilizando la consola

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

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

- [EnableVgwRoutePropagation](#)(API de consultas 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 consultas 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, selecciona Conexiones Site-to-Site VPN.
2. Elija Create VPN Connection (Crear conexión VPN).
3. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión de VPN. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.

4. En Target gateway type (Tipo de puerta de enlace de destino), elija Virtual private gateway (Puerta de enlace privada virtual) o Transit Gateway (Puerta de enlace de tránsito). A continuación, elija la gateway privada virtual o la gateway de tránsito que ha creado anteriormente.
5. En Puerta de enlace de cliente, seleccione Existente y, a continuación, elija la puerta de enlace de cliente que creó anteriormente en ID de puerta de enlace de cliente.
6. Seleccione una de las Opciones de 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 previamente compartida se almacena directamente en el servicio Site-to-Site VPN.
 - Secrets Manager: la clave previamente compartida se almacena mediante AWS Secrets Manager. Para obtener más información acerca de Secrets Manager, consulte [Características de seguridad mejoradas con Secrets Manager](#).
8. Si el tipo de puerta de enlace de destino es una puerta de enlace de tránsito, en la versión Tunnel inside IP, especifique si los túneles VPN admiten IPv4 o no el IPv6 tráfico. IPv6 el tráfico solo es compatible con las conexiones VPN en una puerta de enlace de tránsito.
9. Si especificó IPv4 la versión Túnel dentro de IP, si lo desea, puede especificar los rangos de IPv4 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado es 0.0.0.0/0.

Si ha especificado IPv6 la versión Túnel dentro de IP, también puede especificar los rangos de IPv6 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es ::/0.
10. En Tipo de dirección IP externa, elija una de las siguientes opciones:
 - PublicIPv4: (predeterminado) Usa IPv4 direcciones para el túnel IPs exterior.
 - IPv6- Usa IPv6 direcciones para el túnel exterior IPs. 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 IPv4 CIDR de tamaño /30 del 169.254.0.0/16 rango de las direcciones del túnel IPv4 interior.
 - Si especificó IPv6 para la versión Tunnel inside IP, un bloque IPv6 CIDR /126 del fd00::/8 rango para las direcciones del túnel interno. IPv6
 - La clave previamente compartida de IKE (PSK). Se admiten las siguientes versiones: IKEv1 o. IKEv2
 - Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte [Opciones de túnel de VPN](#).
12. Elija Create VPN Connection (Crear conexión VPN). Es posible que la conexión de VPN tarde unos minutos en crearse.

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

- [CreateVpnConnection](#) (API de consultas de Amazon EC2)
- [create-vpn-connection](#) (AWS CLI)

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

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

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

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

- [New-EC2VpnConnection](#) (AWS Tools for Windows PowerShell)

Paso 6: Descargar el archivo de configuración

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

Important

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

Permisos

Para cargar correctamente la pantalla de configuración de descarga desde Consola de administración de AWS, debe asegurarse de que su rol o usuario de IAM tenga permiso para los siguientes Amazon APIs EC2GetVpnConnectionDeviceTypes: 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 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 Amazon EC2)
- [GetVpnConnectionDeviceSampleConfiguration](#)(API de consultas de Amazon EC2)
- [get-vpn-connection-device-tipos](#) ()AWS CLI
- [get-vpn-connection-device-configuración de muestra](#) ()AWS CLI

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

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

AWS Site-to-Site VPN escenarios arquitectónicos

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

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

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

Varios dispositivos de puerta de enlace del cliente a una única puerta de enlace privada virtual (V)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 la AWS VPN CloudHub. Para obtener más información, consulte [Comunicación segura entre AWS Site-to-Site VPN conexiones mediante VPN CloudHub](#). Si tiene dispositivos de gateway de cliente en distintas ubicaciones geográficas, cada dispositivo debería anunciar un único conjunto de rangos IP específicos de la ubicación.

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

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

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

- [Conexiones de VPN únicas y múltiples](#)
- [the section called “Conexiones de VPN redundantes”](#)
- [Comunicaciones seguras entre conexiones VPN mediante VPN CloudHub](#)

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

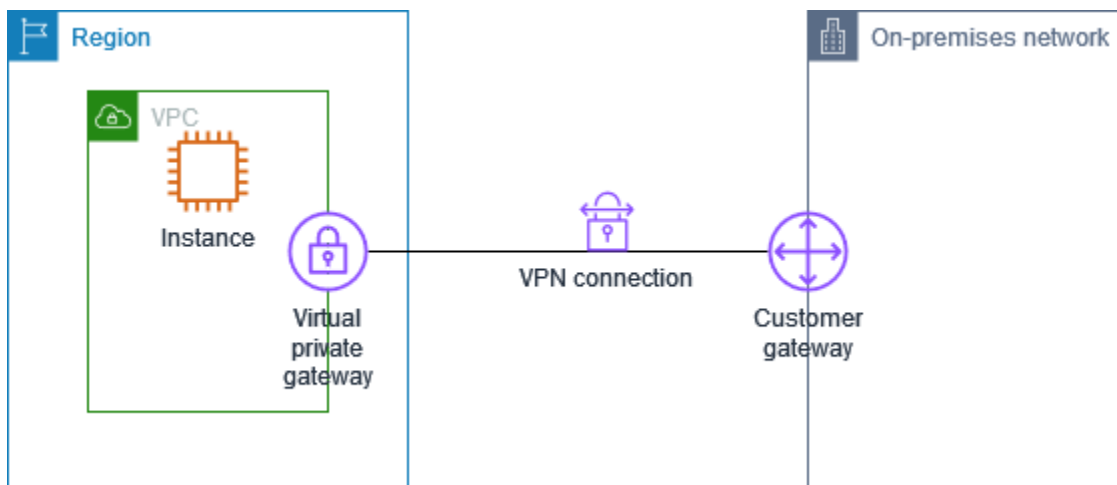
Los siguientes diagramas ilustran las conexiones Site-to-Site VPN únicas y múltiples.

Ejemplos

- [Conexión Site-to-Site VPN única](#)
- [Conexión Site-to-Site VPN única con una puerta de enlace de tránsito](#)
- [Múltiples conexiones Site-to-Site VPN](#)
- [Varias conexiones Site-to-Site VPN con una puerta de enlace de tránsito](#)
- [Site-to-Site Conexión VPN con Direct Connect](#)
- [Conexión Site-to-Site VPN IP privada con Direct Connect](#)

Conexión Site-to-Site VPN única

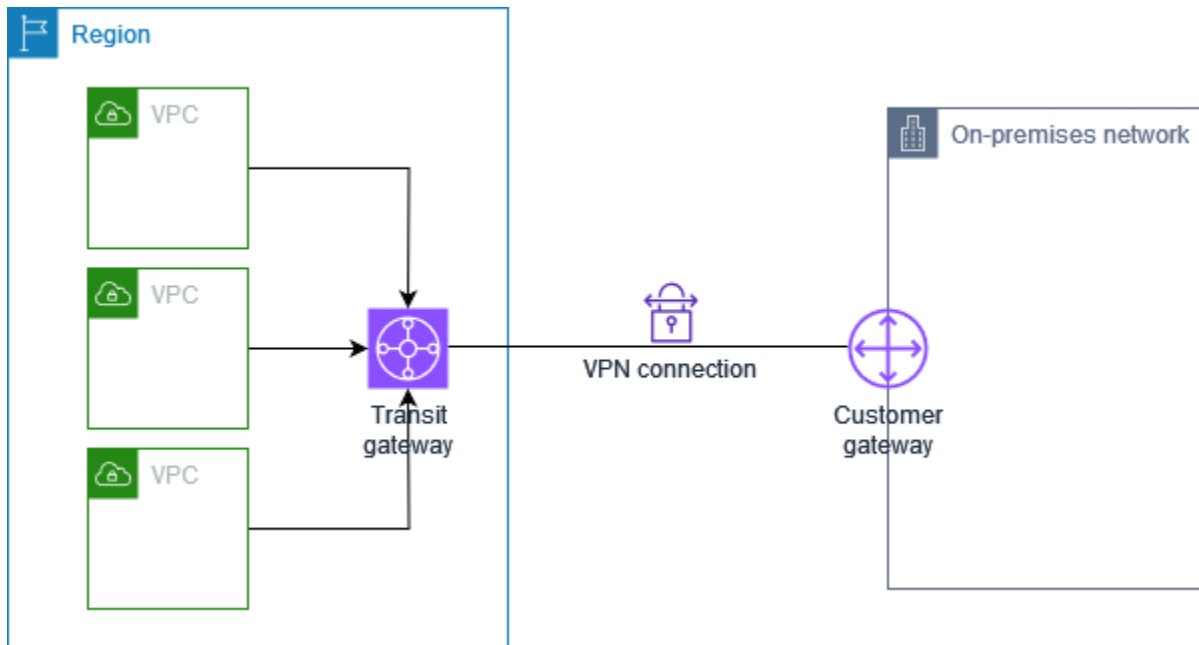
La VPC dispone de una puerta de enlace privada virtual asociada y su red en las instalaciones (remota) incluye un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada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



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

Conexión Site-to-Site VPN única con una puerta de enlace de tránsito

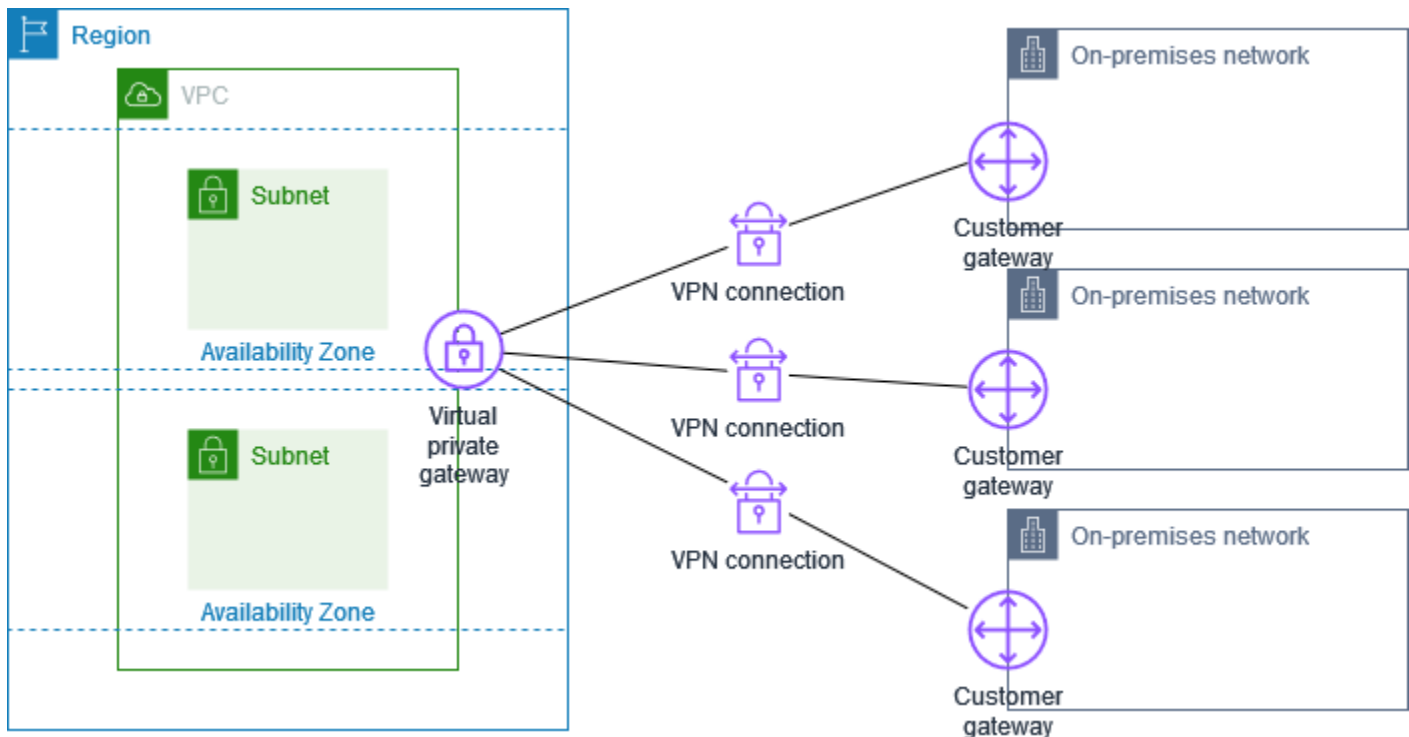
La VPC dispone de una puerta de enlace de tránsito asociada y la red en las instalaciones (remota) contiene un dispositivo de puerta de enlace de cliente que deberá configurar para habilitar la conexión de VPN. Debe configurar tablas de enrutamiento de VPC para que el tráfico procedente de la VPC vinculada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



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

Múltiples conexiones Site-to-Site VPN

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

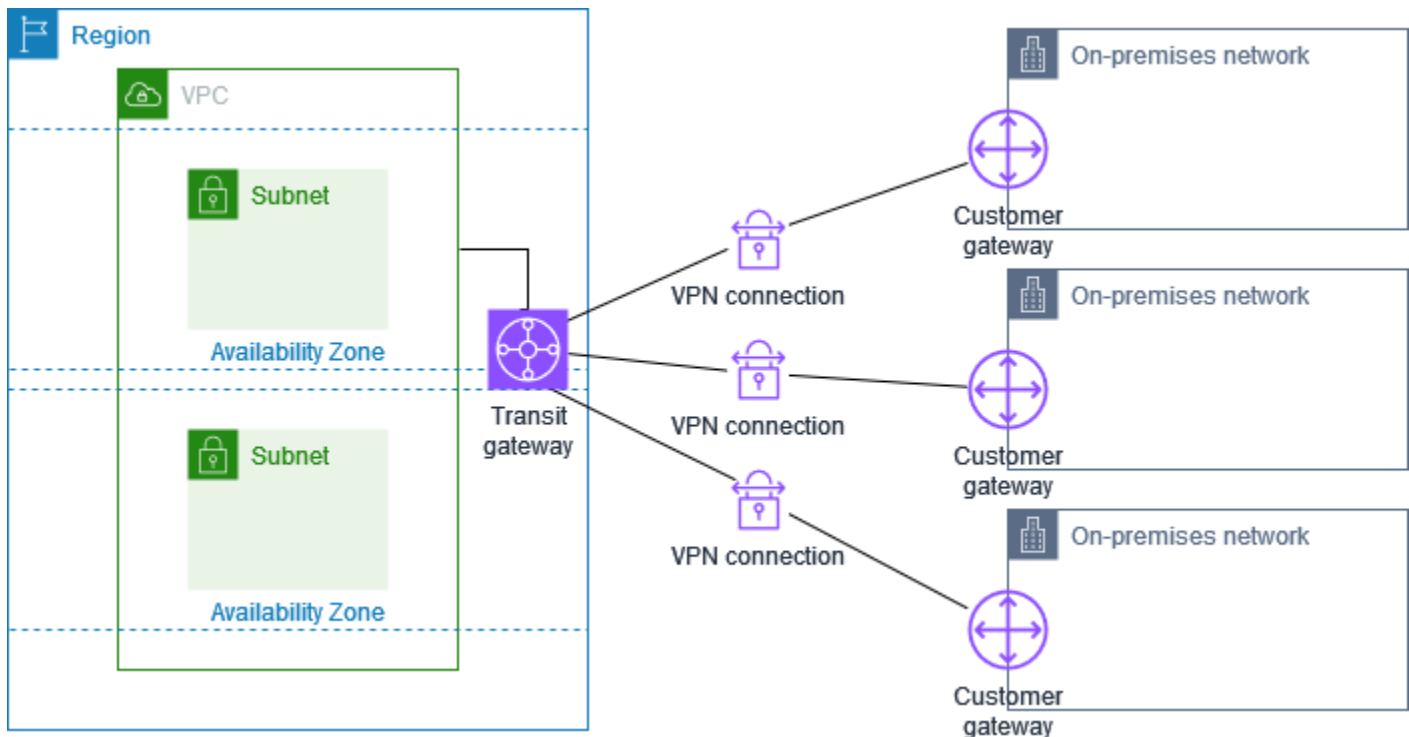


Al crear varias conexiones Site-to-Site VPN a una sola VPC, puede configurar una segunda puerta de enlace de cliente para crear una conexión redundante a la misma ubicación externa. Para obtener más información, consulte [Redundante AWS Site-to-Site VPN conexiones para conmutación por error](#).

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

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

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

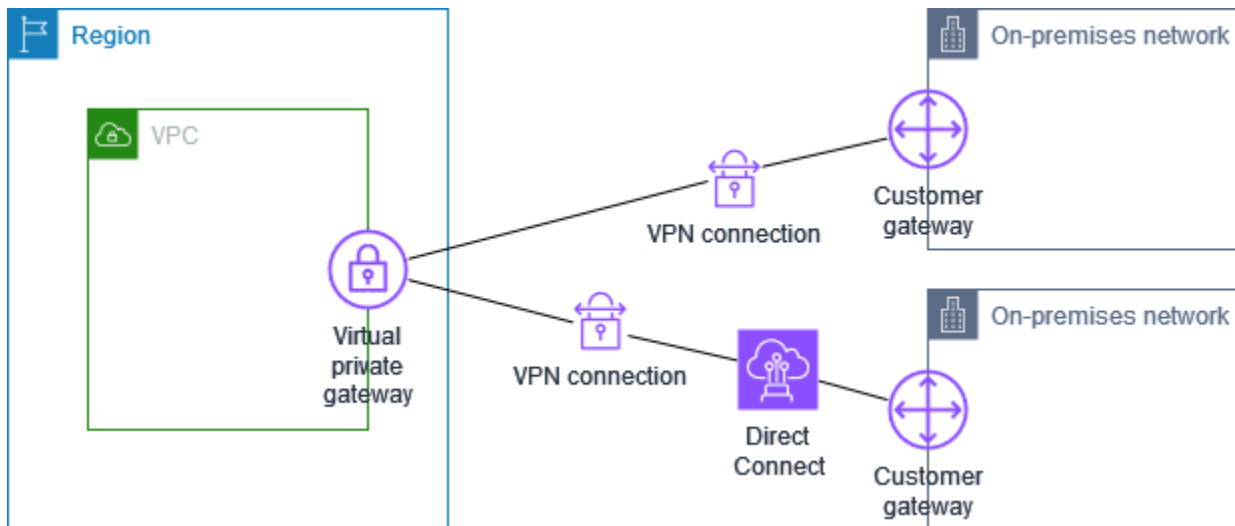


Al crear varias conexiones Site-to-Site VPN a una única puerta de enlace de tránsito, puede configurar una segunda puerta de enlace de cliente para crear una conexión redundante a la misma ubicación externa.

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

Site-to-Site Conexión VPN con Direct Connect

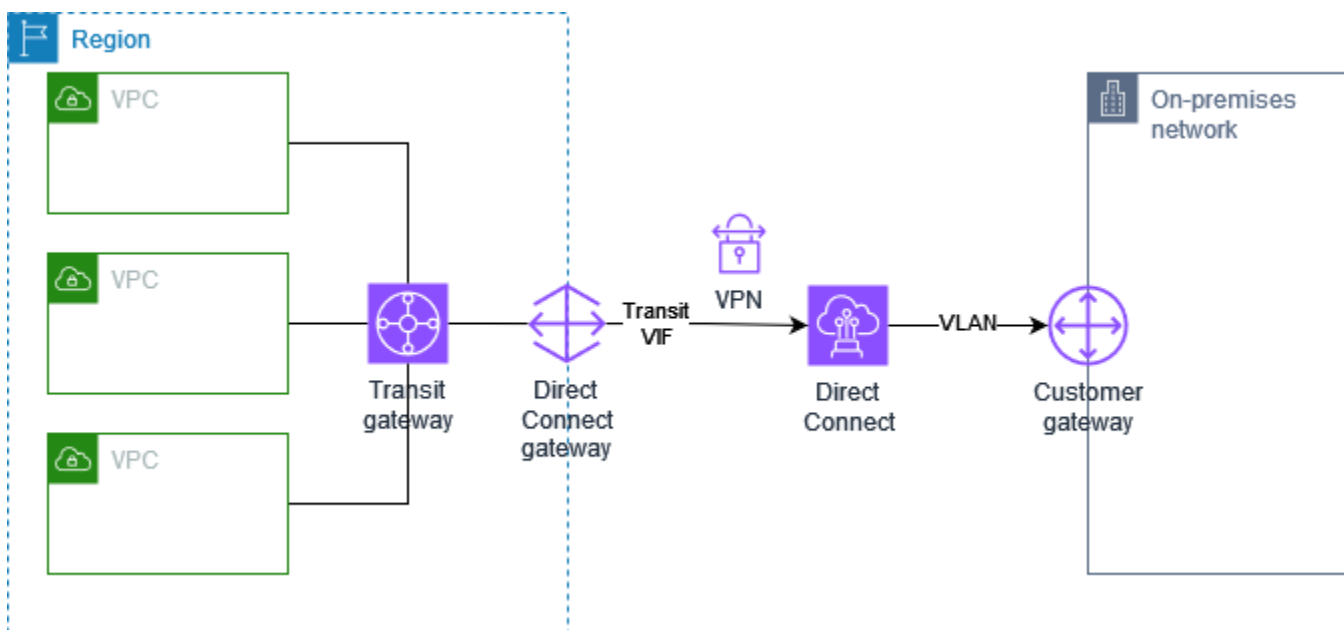
La VPC tiene una puerta de enlace privada virtual adjunta y se conecta a la red local (remota) a través de ella. AWS Direct Connect Puede configurar una interfaz virtual Direct Connect pública para establecer una conexión de red dedicada entre su red y los AWS recursos públicos a través de una puerta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



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

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

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



Para obtener orientación sobre cómo elegir la solución de VPN adecuada, consulte [Selección de la solución de AWS VPN adecuada: un marco de decisión](#).

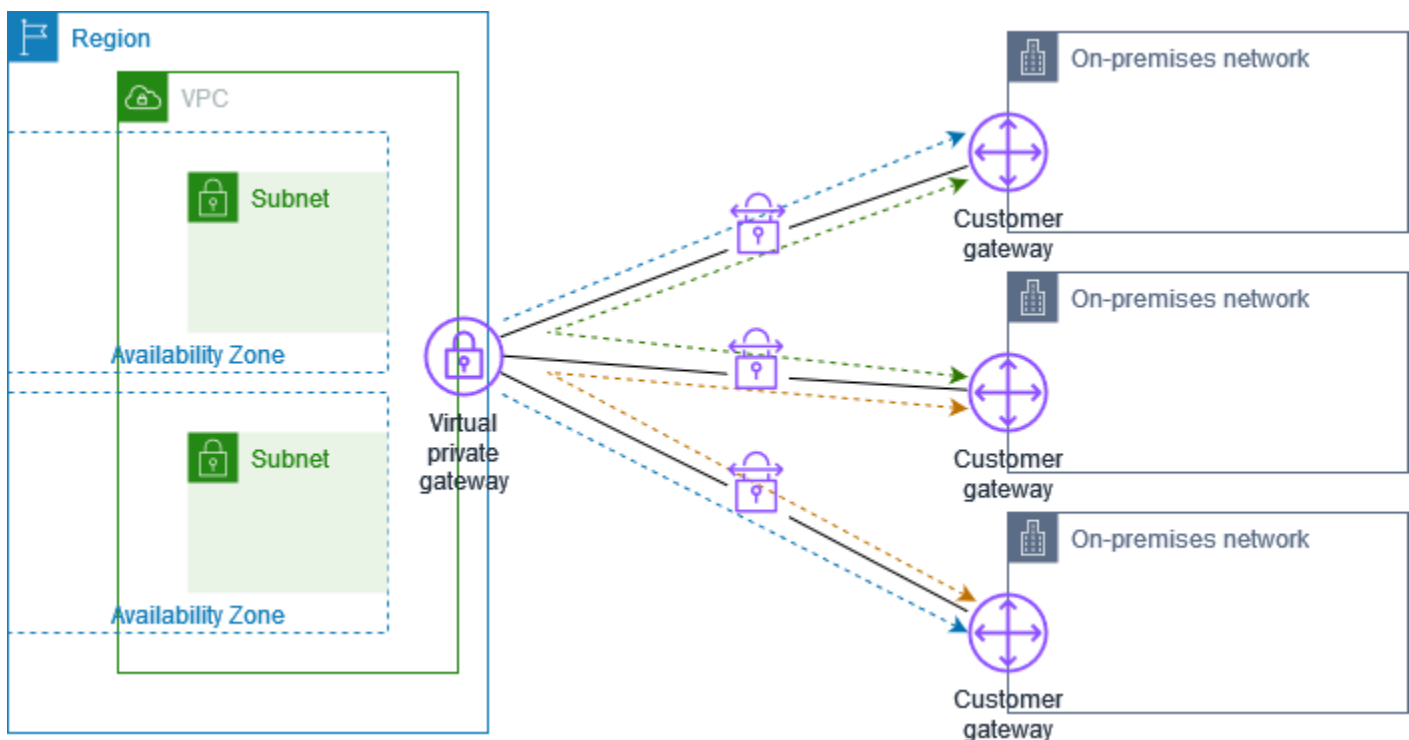
Para obtener más información, consulte la siguiente entrada del blog: [Introducción a las VPN AWS Site-to-Site VPN con IP privada](#).

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

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

Descripción general de

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



En esta situación, haga lo siguiente:

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

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

Precios

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

Por ejemplo, si tiene un sitio en Los Ángeles y un segundo sitio en Nueva York y ambos sitios tienen una conexión Site-to-Site VPN a la puerta de enlace privada virtual, paga la tarifa por hora por cada

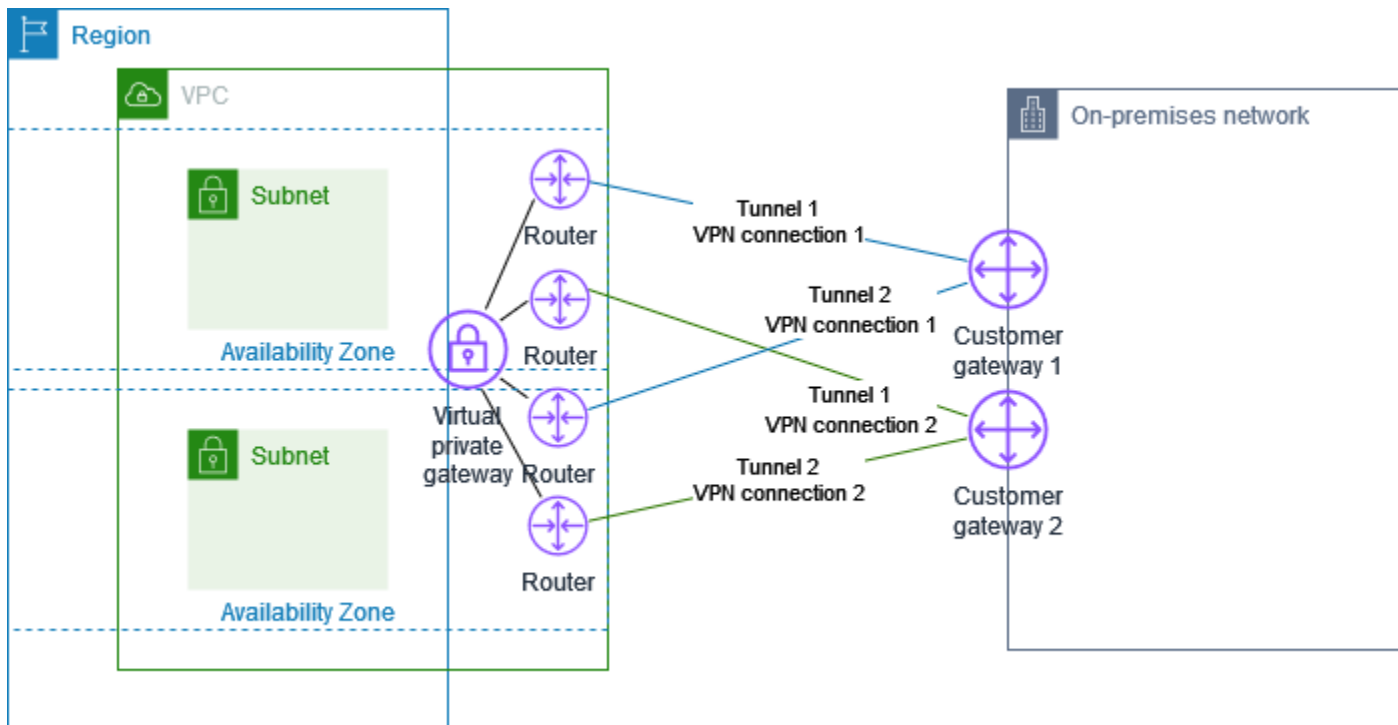
conexión Site-to-Site VPN (por lo que si la tarifa fuera de 0,05\$ por hora, sería un total de 0,10\$ por hora). También pagas las tarifas de transferencia de AWS datos estándar por todos los datos que envíes de Los Ángeles a Nueva York (y viceversa) que atraviesen cada conexión Site-to-Site VPN. El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

Para obtener más información, consulte [Site-to-Site Precios de las conexiones de VPN](#).

Redundante AWS Site-to-Site VPN conexiones para conmutación por error

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

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



En esta situación, haga lo siguiente:

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

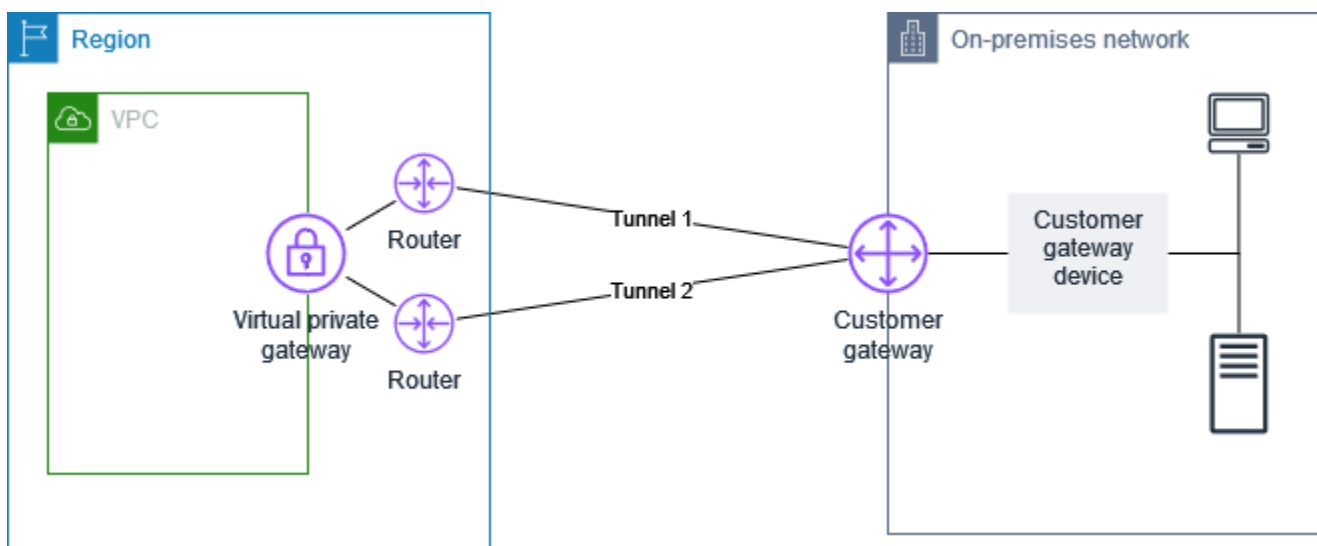
Las conexiones Site-to-Site VPN enrutadas dinámicamente utilizan el protocolo Border Gateway (BGP) para intercambiar información de enrutamiento entre las puertas de enlace de sus clientes y las puertas de enlace privadas virtuales. Las conexiones Site-to-Site VPN con enrutamiento estático requieren que introduzca rutas estáticas para la red remota de su lado de la pasarela del cliente. BGP-advertised y la información de ruta ingresada de forma estática permiten a las puertas de enlace de ambos lados determinar qué túneles están disponibles y redirigir el tráfico en caso de que se produzca una falla. Por lo tanto, se recomienda configurar su red para que utilice la información de direccionamiento que proporciona BGP (si está disponible) y seleccionar una ruta alternativa. La configuración exacta dependerá de la arquitectura de su red.

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

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

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

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



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

También puede encontrar dispositivos de VPN por software en [AWS Marketplace](#).

Requisitos para un AWS Site-to-Site VPN Dispositivo de gateway de cliente

AWS es compatible con varios dispositivos Site-to-Site VPN de puerta de enlace para clientes, para los que proporcionamos archivos de configuración descargables. Para obtener una lista de 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 figura en la lista de dispositivos compatibles, en la siguiente sección se describen los requisitos que debe cumplir el dispositivo para establecer una conexión Site-to-Site VPN.

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

	Asociación de seguridad de intercambio de claves de Internet (IKE). Necesaria para intercambiar claves utilizadas para establecer la asociación de seguridad de IPsec.
	Asociación de seguridad IPsec. Gestiona el cifrado del túnel, la autenticación, etc.
	Interfaz de túnel. Recibe el tráfico entrante y saliente del túnel.
	(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. En su lugar, puede configurar la conexión VPN para que inicie la negociación del IKE desde el AWS lado de la conexión. Para obtener más información, consulte [AWS Site-to-Site VPN opciones de inicio de túnel](#).

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

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

Requisito	RFC	Comentarios
		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 	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.
Utilice la función de SHA-1 hash or SHA-2 (256)	RFC 2404	Esta función de hash se utiliza para autenticar asociaciones de seguridad de IKE y de IPsec.
Utilice Diffie-Hellman Perfect Forward Secrecy.	RFC 2409	IKE utiliza claves efímeras Diffie-Hellman para proteger todas las comunicaciones entre los dispositivos de puerta de enlace del cliente y las puertas de enlace 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 Dynamically-routed VPN) Utilice la detección IPsec Dead Peer	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 Dynamically-routed VPN) Enlaza el túnel a la interfaz lógica (VPN basada en rutas)	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 Dynamically-routed VPN) Establezca pares 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.

Tunnel

BGP

[Una conexión AWS VPN no admite Path MTU Discovery \(RFC 1191\).](#)

Si tiene un firewall entre el dispositivo de gateway de cliente e Internet, consulte [Reglas de firewall para un AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

Prácticas recomendadas para un AWS Site-to-Site VPN Dispositivo de gateway de cliente

Uso de IKEv2

Le recomendamos encarecidamente que utilice IKEv2 para su Site-to-Site conexión 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 su conexión Site-to-Site VPN superan el tamaño de la MTU, deben estar fragmentados. Para evitar una disminución del rendimiento, le recomendamos que configure el dispositivo de puerta de enlace del cliente para fragmentar los paquetes antes de cifrarlos. Site-to-Site A continuación, la 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. AWS Consulte [RFC 4459](#) para obtener más información.

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

Como la Site-to-Site VPN reagrupará todos los paquetes fragmentados recibidos desde el dispositivo de puerta de enlace del cliente antes de reenviarlos al siguiente destino, tenga en cuenta que es posible que haya que tener en cuenta los paquetes size/MTU en las redes de destino a las que se reenvíen después, por ejemplo, a través de determinados protocolos, como Radius Direct Connect.

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

Los paquetes TCP suelen ser el tipo de paquete más común en los túneles de IPsec. Site-to-Site La VPN admite una unidad de transmisión máxima (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 cómo evitar la fragmentación y MTU/MSS lograr un rendimiento óptimo:

Algoritmo de cifrado	Algoritmo hash	NAT-Traversal	MTU	MSS (IPv4)	MSS () IPv6-in-IPv4
AES-GCM-16	N/A	disabled	146	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 AES-GCM algoritmos cubren tanto el cifrado como la autenticación, por lo que no existe una opción de algoritmo de autenticación distinta que pueda afectar 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 AWS Site-to-Site VPN Dispositivo de gateway de cliente

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

Entrante (de Internet)

Regla de entrada I1

IP de origen	IP externa de Tunnel1
IP destino	Gateway de cliente
Protocolo	UDP
Puerto de origen	500
Destino	500

Regla de entrada I2

IP de origen	IP externa de Tunnel2
IP destino	Gateway de cliente
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500

Regla de entrada I3

IP de origen	IP externa de Tunnel1
IP destino	Gateway de cliente

Protocolo	IP 50 (ESP)
Regla de entrada I4	
IP de origen	IP externa de Tunnel2
IP destino	Gateway de cliente
Protocolo	IP 50 (ESP)
Saliente (a Internet)	
Regla de salida O1	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel1
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de salida O2	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel2
Protocolo	UDP
Puerto de origen	500
Puerto de destino	500
Regla de salida O3	
IP de origen	Gateway de cliente
IP destino	IP externa de Tunnel1

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

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

Note

Si utiliza NAT traversal (NAT-T) en su dispositivo, asegúrese de que el tráfico UDP del puerto 4500 también pueda pasar entre la red y los AWS Site-to-Site VPN puntos finales. Comprueba si tu dispositivo tiene publicidad. NAT-T

Archivos de configuración estáticos y dinámicos para un AWS Site-to-Site VPN Dispositivo de gateway de cliente

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

⚠ Important

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

ℹ Note

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

La 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
PUERTA HEXAGONAL	NF	LAOS 3.2+
PUERTA AXGATE	UTM	LAOS 2.1+
Punto de comprobación	Gaia	R80.10+
Cisco Meraki	Serie MX	15.12+ (WebUI)
Cisco Systems, Inc.	Serie ASA 5500	ASA 9.7+ VTI

Proveedor	Plataforma	Software
Cisco Systems, Inc.	AMI CSrV	IOS 12.4+
Fortinet	Serie Fortigate 40+	ForTIOS 6.4.4+ (GUI)
Juniper Networks, Inc.	J-Series Enrutadores	JunOS 9.5+
Juniper Networks, Inc.	Routers SRX	JunOS 11.0+
Mikrotik	RouterOS	6.44.3
Palo Alto Networks	Serie PA	PANOS 7.0+
SonicWall	NSA, TZ	OS 6.5
Sophos	Sophos Firewall	v19+
Strongswan	Ubuntu 16.04	Strongswan 5.5.1+
Yamaha	Routers RTX	Rev.10.01.16+

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

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

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

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

- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual

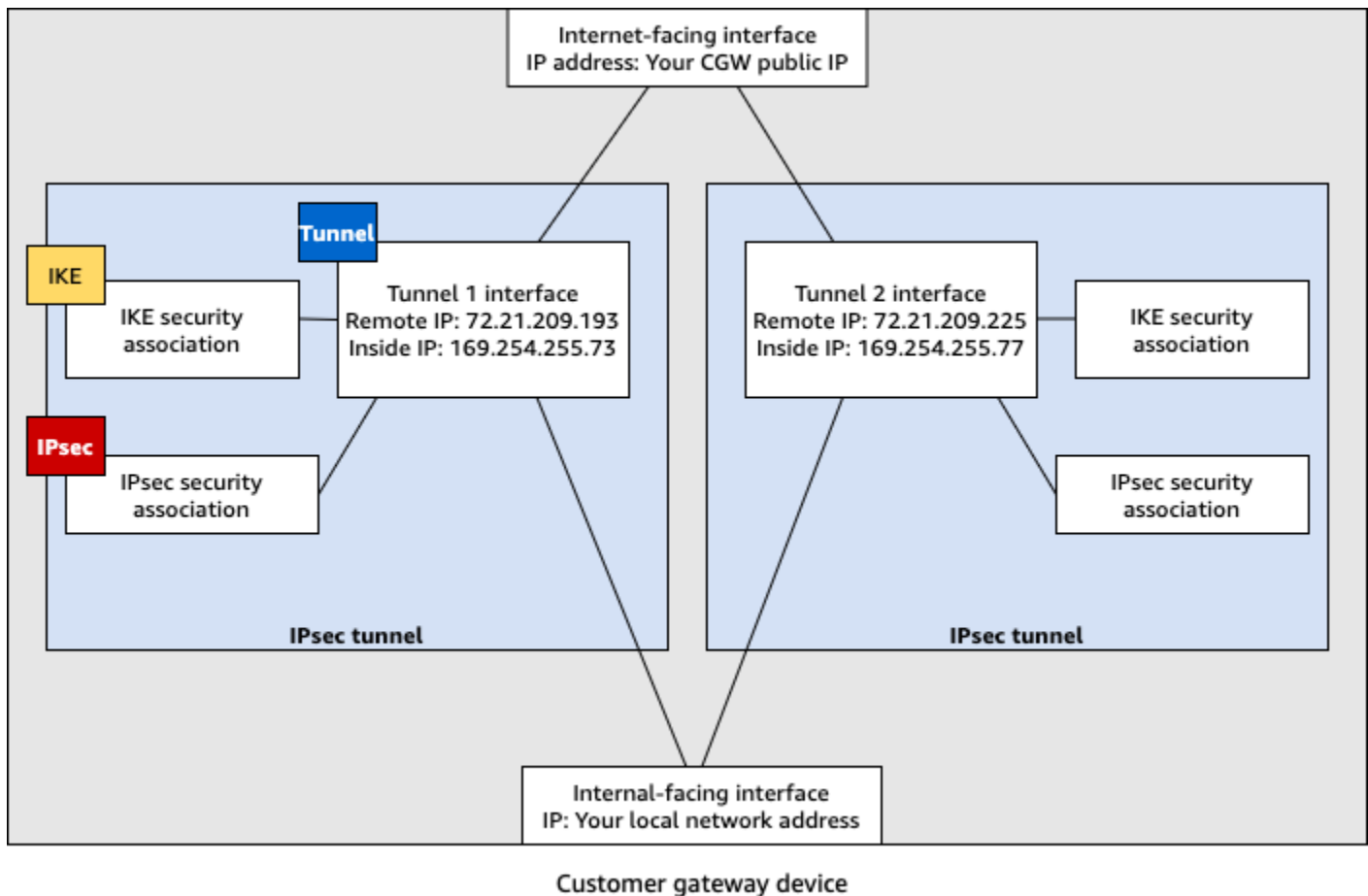
- Marcadores de posición para los AWS puntos finales de la dirección IP remota (externa) (y) *AWS_ENDPOINT_1 AWS_ENDPOINT_2*
- Un marcador de posición para la dirección IP de la interfaz externa enrutable a Internet del dispositivo de pasarela del cliente () *your-cgw-ip-address*
- Un marcador de posición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

Note

La configuración de MTU proporcionada en los archivos de configuración de muestra son solo ejemplos. Consulte [Prácticas recomendadas para un AWS Site-to-Site VPN Dispositivo de gateway de cliente](#) para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

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

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



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

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

Check Point

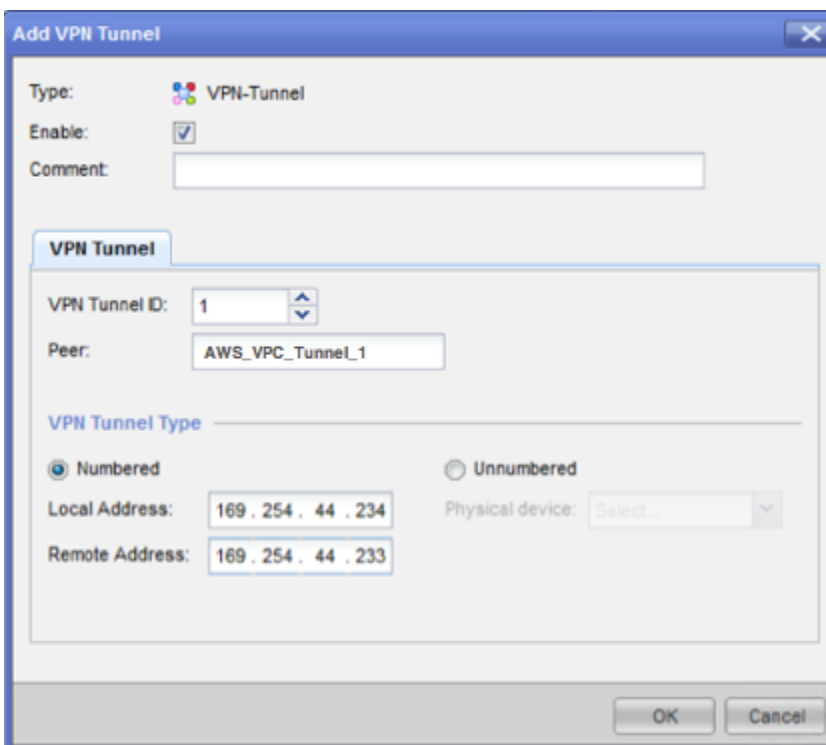
Los siguientes son los pasos para configurar su dispositivo de pasarela de clientes si su dispositivo es un dispositivo Check Point Security Gateway que ejecute R77.10 o superior y utilice el sistema operativo Gaia y Check Point. SmartDashboard También puede consultar el artículo de [Check Point Security Gateway IPsec VPN to Amazon Web Services VPC](#) en el Check Point Support Center.

Para configurar la interfaz de túnel

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

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

1. Abra el portal de Gaia de su dispositivo Check Point Security Gateway.
2. Elija Network Interfaces, Add, VPN tunnel.
3. En el cuadro de diálogo, configure los ajustes tal como se muestra y elija OK cuando haya terminado:
 - Para VPN Tunnel ID, escriba cualquier valor único, como 1.
 - Para Peer, escriba un nombre único para cada túnel, como AWS_VPC_Tunnel_1 o AWS_VPC_Tunnel_2.
 - Asegúrese de que la opción Numbered (Numerado) esté seleccionada y, en Local Address (Dirección local), escriba la dirección IP especificada para CGW Tunnel IP en el archivo de configuración; por ejemplo: 169.254.44.234.
 - Para Remote Address, escriba la dirección IP especificada para VGW Tunnel IP en el archivo de configuración; por ejemplo: 169.254.44.233.



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

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

```
set interface vpnt1 mtu 1436
```

Para el túnel 2, ejecute el siguiente comando:

```
set interface vpnt2 mtu 1436
```

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

Para configurar las rutas estáticas

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

1. En el portal de Gaia, seleccione Rutas IPv4 estáticas y añada.
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.

Edit Destination Route: 10.28.13.0/24

Destination: 10.28.13.0/24

Next Hop Type: Normal

Normal: Accept and forward packets.
Reject: Drop packets, and send *unreachable* messages.
Black Hole: Drop packets, but don't send *unreachable* messages.

Rank: Default: 60

Local Scope: ☐

Comment:

Add Gateway

Ping: ☐

Add Gateway Edit Delete

Gateway	Priority
169.254.44.233	1
169.254.44.5	2

Save Cancel

7. Seleccione Save.

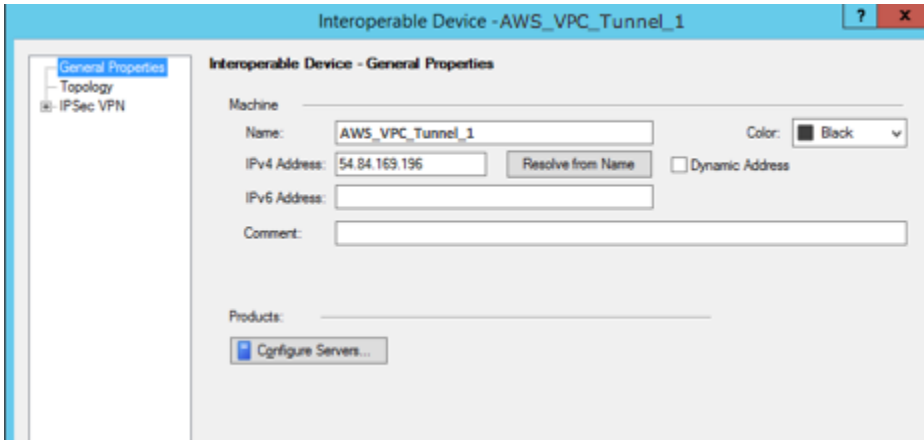
Si va a utilizar un clúster, repita los pasos anteriores para los demás miembros del clúster.

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. Abre el punto SmartDashboard de control.
2. Para Groups, abra el menú contextual y elija Groups, Simple Group. Puede utilizar el mismo grupo para cada objeto de red.
3. Para Network Objects, abra el menú contextual (clic con el botón derecho) y elija New, Interoperable Device.
4. Para Name (Nombre), escriba el nombre que ha proporcionado para cada túnel, por ejemplo: AWS_VPC_Tunnel_1_1 o AWS_VPC_Tunnel_1_2.

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



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

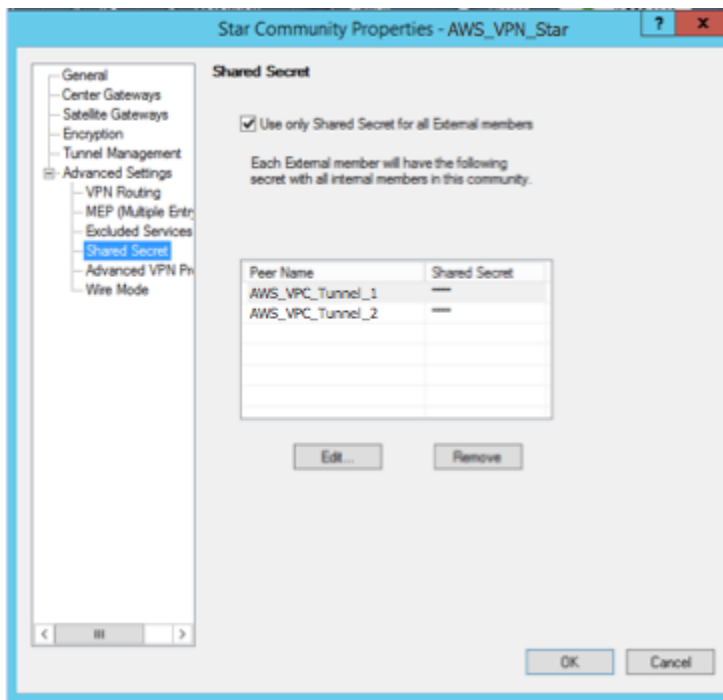
Note

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 la comunidad VPN, el IKE y los ajustes IPsec

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

1. En las propiedades de la puerta de enlace, elija IPSecVPN en el panel de categorías.
2. Elija Communities, New, Star Community.
3. Proporcione un nombre para su comunidad (por ejemplo, AWS_VPN_Star) y, a continuación, elija Center Gateways en el panel Category.
4. Elija Add y agregue su gateway o clúster a la lista de gateways participantes.
5. En el panel Category (Categoría), elija Satellite Gateways (Gateways satélite), Add (Agregar), y luego agregue los dispositivos interoperables que creó anteriormente (AWS_VPC_Tunnel_1 y AWS_VPC_Tunnel_2) a la lista de gateways participantes.
6. En el panel Category, elija Encryption. En la sección Método de cifrado, elija IKEv1 solo. En la sección Encryption Suite, elija Custom, Custom Encryption.
7. En el cuadro de diálogo, configure las propiedades de cifrado tal como se muestra y elija OK cuando haya terminado:
 - Propiedades de asociación de seguridad de IKE (fase 1):
 - Perform key exchange encryption with: AES-128
 - Perform data integrity with: SHA-1
 - IPsec Propiedades de la asociación de seguridad (fase 2):
 - Realice el cifrado IPsec de datos con: AES-128
 - Perform data integrity with: SHA-1
8. En el panel Category, elija Tunnel Management. Elija Set Permanent Tunnels, On all tunnels in the community. En la sección VPN Tunnel Sharing, elija One VPN tunnel per Gateway pair.
9. En el panel Category, expanda Advanced Settings y elija Shared Secret.
10. Seleccione el nombre homólogo para el primer túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección IPSec Tunnel #1 del archivo de configuración.
11. Seleccione el nombre homólogo para el segundo túnel, elija Edit (Editar) y escriba la clave previamente compartida según lo especificado en la sección IPSec Tunnel #2 del archivo de configuración.



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

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

Para crear reglas de firewall

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

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

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

Para modificar la propiedad `tunnel_keepalive_method`

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

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

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

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

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

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

Para habilitar el bloqueo TCP MSS

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

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

Para verificar el estado del túnel

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

```
vpn tunnelutil
```

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

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

Log Info		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695		
Traffic		More	
Source	Management_PC (192.168.1.116)	Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Destination	10.28.13.28	Community	AWS_VPN_Star
Service	---	Encryption Scheme	IKE
Protocol	icmp	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Interface	eth0	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Source Port	---	Subproduct	VPN
		VPN Feature	VPN
		Product Family	Network
		Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy			
Policy Name	Standard		
Policy Date	Tue Nov 03 11:33:45 2015		
Policy Management	cpgw-997695		

SonicWALL

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

Para configurar los túneles

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

- Policy Type (Tipo de política): seleccione Tunnel Interface (Interfaz de túnel).
 - Authentication Method: elija IKE using Preshared Secret.
 - Name: escriba un nombre para la política de VPN. Le recomendamos utilizar el nombre del ID de VPN tal como se indica en el archivo de configuración.
 - IPsec Nombre o dirección de la puerta de enlace principal: introduzca la dirección IP de la puerta de enlace privada virtual tal como se indica en el archivo de configuración (por ejemplo, 72.21.209.193).
 - IPsec Nombre o dirección de la puerta de enlace secundaria: deje el valor predeterminado.
 - Shared Secret: escriba la clave previamente compartida tal como se indica en el archivo de configuración y vuelva a escribirla en Confirm Shared Secret.
 - ID IKE local: introduzca la IPv4 dirección de la pasarela del cliente (el dispositivo SonicWall).
 - ID IKE del mismo nivel: introduzca la IPv4 dirección de la puerta de enlace privada virtual.
4. En la pestaña Network, complete la información siguiente:
- En Local Networks, elija Any address. Se recomienda utilizar esta opción para evitar problemas de conectividad en su red local.
 - En Remote Networks, elija Choose a destination network from list. Cree un objeto de dirección con el CIDR de su VPC en AWS.
5. En la pestaña Proposals (Propuestas), complete la información siguiente:
- En IKE (Phase 1) Proposal, haga lo siguiente:
 - Exchange: elija Main Mode.
 - DH Group (Grupo de DH): escriba un valor para el grupo Diffie-Hellman (por ejemplo, 2).
 - Encryption: elija AES-128 o AES-256.
 - Autenticación: elija SHA1o SHA256.
 - Life Time: escriba 28800.
 - En IKE (Phase 2) Proposal, haga lo siguiente:
 - Protocol: elija ESP.
 - Encryption: elija AES-128 o AES-256.
 - Autenticación: elija SHA1o SHA256.

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

 Important

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

6. En la pestaña Advanced, complete la información siguiente:
 - Seleccione Enable Keep Alive.
 - Seleccione Enable Phase2 Dead Peer Detection y escriba lo siguiente:
 - En Dead Peer Detection Interval, escriba 60 (este es el valor mínimo que puede aceptar el dispositivo SonicWALL).
 - En Failure Trigger Level, escriba 3.
 - En VPN Policy bound to, seleccione Interface X1. Esta es la interfaz que suele designarse para las direcciones IP públicas.
7. Seleccione 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

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

Cisco ASAs a partir de la versión 9.7.1 y del Active/Active modo de soporte posterior. Al utilizar estos sistemas Cisco ASAs, puede tener ambos túneles activos al mismo tiempo. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Para los dispositivos Cisco, debe hacer lo siguiente:

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

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

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

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

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

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

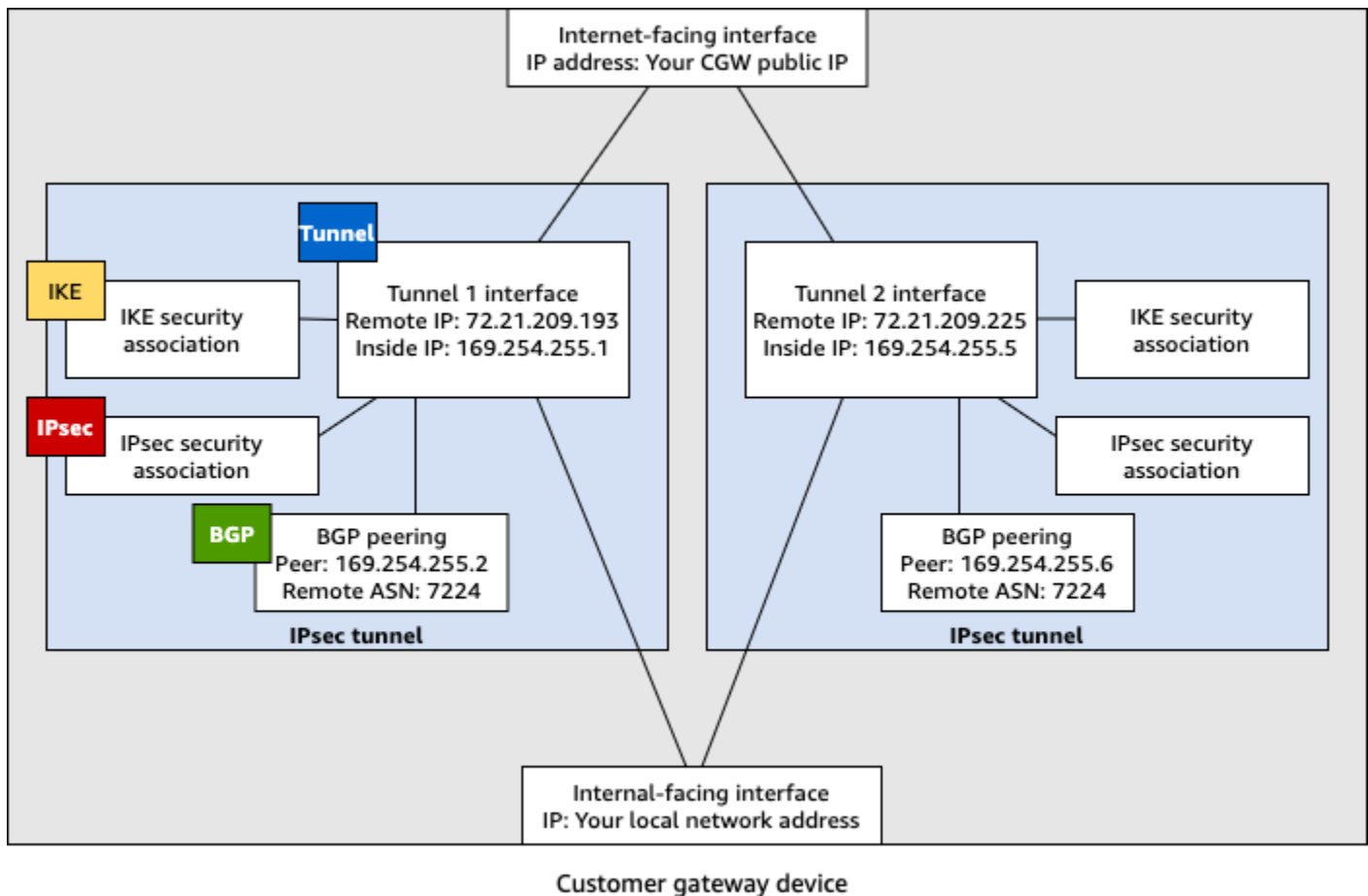
- Valores de ejemplo para el ID de conexión de VPN, el ID de gateway de cliente y el ID de gateway privada virtual
- Marcadores de posición para los AWS puntos finales de la dirección IP remota (externa) (y) *AWS_ENDPOINT_1 AWS_ENDPOINT_2*
- Un marcador de posición para la dirección IP de la interfaz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

Note

La configuración de MTU proporcionada en los archivos de configuración de muestra son solo ejemplos. Consulte [Prácticas recomendadas para un AWS Site-to-Site VPN Dispositivo de gateway de cliente](#) para obtener información sobre cómo establecer el valor de MTU óptimo para su situación.

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

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



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

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

Check Point

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

Para configurar la interfaz de túnel

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

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

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

```
set as 65000
```

3. Cree la interfaz del primer túnel utilizando la información que se proporciona en la sección IPsec Tunnel #1 del archivo de configuración. Especifique un nombre exclusivo para su túnel como, por ejemplo, `AWS_VPC_Tunnel_1`.

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

4. Repita estos comandos para crear el segundo túnel utilizando la información que se proporciona en la sección IPsec Tunnel #2 del archivo de configuración. Especifique un nombre exclusivo para su túnel como, por ejemplo, `AWS_VPC_Tunnel_2`.

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

5. Establezca el ASN de la gateway privada virtual.

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

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

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

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

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

8. Guarde la configuración.

```
save config
```

Para crear una política de BGP

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

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

Para anunciar rutas locales

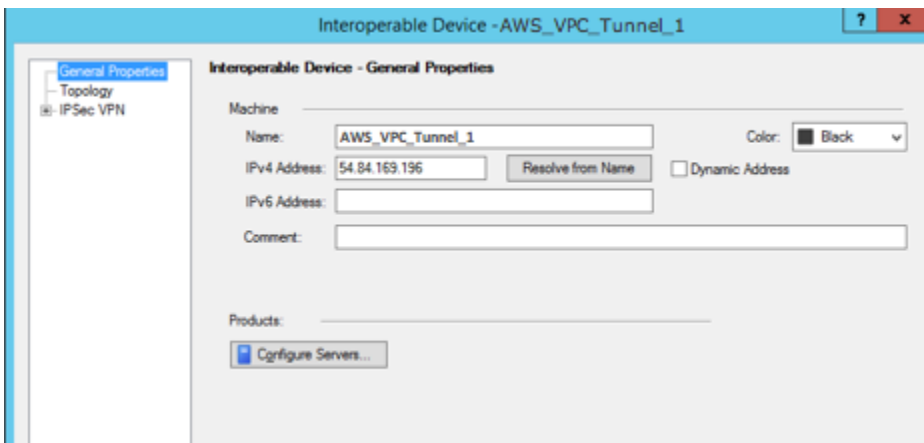
A continuación se presentan los pasos para distribuir rutas de interfaces locales. También puede redistribuir rutas desde distintos orígenes (por ejemplo, rutas estáticas o rutas obtenidas mediante protocolos de direccionamiento dinámico). Para obtener más información, consulte la [Gaia Advanced Routing 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 el punto de control. SmartDashboard
2. Para Groups, abra el menú contextual y elija Groups, Simple Group. Puede utilizar el mismo grupo para cada objeto de red.
3. Para Network Objects, abra el menú contextual (clic con el botón derecho) y elija New, Interoperable Device.
4. En Name (Nombre), escriba el nombre que ha proporcionado para el túnel en el paso 1, por ejemplo: AWS_VPC_Tunnel_1 o AWS_VPC_Tunnel_2.
5. En IPv4 Dirección, introduzca la dirección IP externa de la puerta de enlace privada virtual proporcionada en el archivo de configuración, por ejemplo, 54.84.169.196. Guarde la configuración y cierre el cuadro de diálogo.



6. En el panel de categorías izquierdo, elija Topology.
7. En la sección VPN Domain (Dominio de VPN), elija Manually defined (Definido manualmente), desplácese hasta el grupo sencillo vacío que creó en el paso 2 y selecciónelo. Seleccione 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 la comunidad VPN, el IKE y los IPsec ajustes

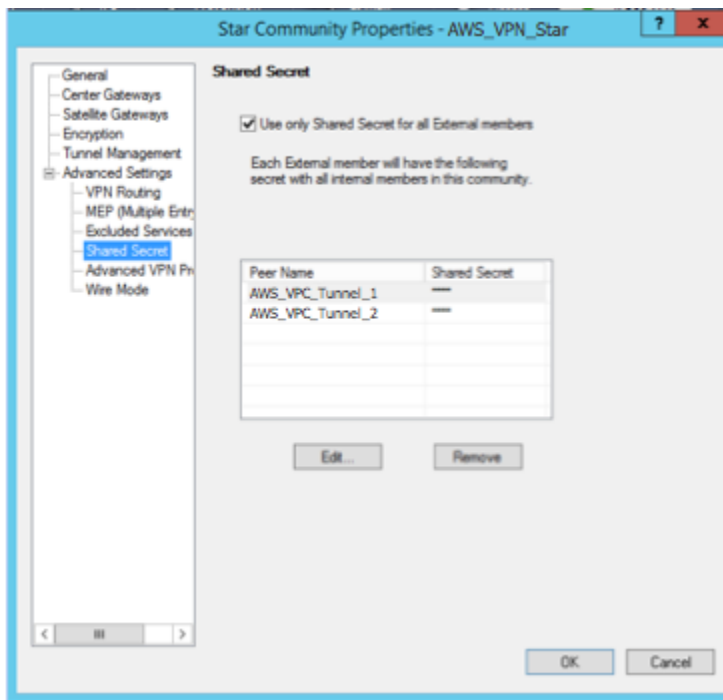
A continuación, cree una comunidad de VPN en su gateway de Check Point, a la que agregará los objetos de red (dispositivos interoperables) para cada túnel. También puede configurar el intercambio de claves de Internet (IKE) y los IPsec ajustes.

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

 Note

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

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



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

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

Para crear reglas de firewall

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

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

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

Para modificar la propiedad `tunnel_keepalive_method`

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

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

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

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

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

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

Para habilitar el bloqueo TCP MSS

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

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

Para verificar el estado del túnel

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

```
vpn tunnelutil
```

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

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

Log Info		Rule	
Product	Security Gateway/Management	Action	Encrypt
Date	4Nov2015	Rule	4
Time	9:42:01	Current Rule Number	4-Standard
Number	21254	Rule Name	---
Type	Log	User	---
Origin	cpgw-997695		
Traffic		More	
Source	Management_PC (192.168.1.116)	Rule UID	{0AA18015-FF7B-4650-B0CE-3989E658CF04}
Destination	10.28.13.28	Community	AWS_VPN_Star
Service	---	Encryption Scheme	IKE
Protocol	icmp	Data Encryption Methods	ESP: AES-128 + SHA1 + PFS (group 2)
Interface	eth0	VPN Peer Gateway	AWS_VPC_Tunnel_1 (54.84.169.196)
Source Port	---	Subproduct	VPN
Policy		VPN Feature	VPN
Policy Name	Standard	Product Family	Network
Policy Date	Tue Nov 03 11:33:45 2015	Information	service_id: icmp-proto ICMP: Echo Request ICMP Type: 8 ICMP Code: 0
Policy Management	cpgw-997695		

SonicWALL

Puede configurar el dispositivo SonicWALL mediante la interfaz de administración de SonicOS. Para obtener más información sobre la configuración de los túneles, consulte [Configure el enrutamiento estático para un dispositivo de puerta de enlace del cliente 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 ASAs solo admiten el Active/Standby modo Cisco. Cuando utiliza estos Cisco ASAs, solo puede tener un túnel activo a la vez. El otro túnel en espera se activará si el primer túnel se vuelve no disponible. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Cisco ASAs a partir de la versión 9.7.1 y del Active/Active modo de soporte posterior. Al utilizar estos sistemas Cisco ASAs, puede tener ambos túneles activos al mismo tiempo. Con esta redundancia, siempre debería tener conectividad a su VPC a través de uno de los túneles.

Para los dispositivos Cisco, debe hacer lo siguiente:

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

Dispositivos Juniper: información adicional

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

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

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

Puede configurar el servidor que ejecute Windows Server como dispositivo de gateway de cliente para la VPC. Utilice el siguiente proceso tanto si ejecuta Windows Server en una 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](#)
- [Paso 1: Crear una conexión de VPN y configurar la VPC](#)
- [Paso 2: Descargar el archivo de configuración de la conexión de VPN](#)
- [Paso 3: Configuración de Windows Server](#)
- [Paso 4: Configurar el túnel de VPN](#)
- [Paso 5: Habilitar la detección de gateways inactivas](#)
- [Paso 6: Comprobar la conexión de VPN](#)

Configuración de instancias de Windows

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

- Inhabilita la source/destination comprobación de 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 Avanzadas, deshabilita las propiedades IPv4Checksum Offload, TCP Checksum Offload (IPv4) y UDP Checksum Offload () y, a continuación, selecciona Aceptar. IPv4
- Asigne una dirección IP elástica a su cuenta y asóciela a la instancia. Para obtener más información, consulte [Direcciones IP elásticas](#) en la Guía del 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 la instancia permitan el tráfico saliente. IPsec De forma predeterminada, un grupo de seguridad permite todo el tráfico saliente. Sin embargo, si las reglas de salida del grupo de seguridad se han modificado con respecto a su estado original, debe crear las siguientes reglas de protocolo de salida personalizadas para el IPsec tráfico: protocolo IP 50, protocolo IP 51 y UDP 500.

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

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

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

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

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

Para configurar la VPC

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

 Note

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

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

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

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

Cómo descargar el archivo de configuración

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

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

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

Local Tunnel Endpoint

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

Remote Tunnel Endpoint

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

Endpoint 1

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

Endpoint 2

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

Preshared key

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

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

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

Note

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

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

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

MainModeSecMethods

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

MainModeKeyLifetime

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

QuickModeSecMethods

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

QuickModePFS

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

Paso 3: Configuración de Windows Server

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

Para instalar servicios de direccionamiento y acceso remoto

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

Para configurar y habilitar el servidor de enrutamiento y acceso remoto

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

Paso 4: Configurar el túnel de VPN

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

Important

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

Opciones

- [Opción 1: ejecutar el script netsh](#)
- [Opción 2: utilizar la interfaz de usuario del servidor de Windows](#)

Opción 1: ejecutar el script netsh

Copie el script netsh del archivo de configuración descargado y reemplace las variables. A continuación se muestra un ejemplo de script.

```
netsh advfirewall consec add rule Name="vgw-1a2b3c4d Tunnel 1" ^
```

```
Enable=Yes Profile=any Type=Static Mode=Tunnel ^
LocalTunnelEndpoint=Windows_Server_Private_IP_address ^
RemoteTunnelEndpoint=203.83.222.236 Endpoint1=Your_Static_Route_IP_Prefix ^
Endpoint2=Your_VPC_CIDR_Block Protocol=Any Action=RequireInClearOut ^
Auth1=ComputerPSK Auth1PSK=xCjNLsLoCmKsawkcdR9yX6GsEXAMPLE ^
QMSecMethods=ESP:SHA1-AES128+60min+100000kb ^
ExemptIPsecProtectedConnections=No ApplyAuthz=No QMPFS=dhgroup2
```

Name: puede sustituir el nombre recomendado (vgw-1a2b3c4d Tunnel 1) por el nombre que prefiera.

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

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

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

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

Cuando haya terminado, vaya a [Configurar el firewall de Windows](#).

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

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

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

Important

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

Tareas

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

Configurar una regla de seguridad para un túnel VPN

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

Para configurar una regla de seguridad para un túnel de VPN

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

⚠ Important

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

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

⚠ Important

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

The screenshot shows the 'New Connection Security Rule Wizard' window, specifically the 'Tunnel Endpoints' step. The window has a blue title bar and a sidebar on the left with a 'Steps' list: Rule Type, Tunnel Type, Requirements, Tunnel Endpoints (selected), Authentication Method, Profile, and Name. The main area is titled 'Specify the endpoints for the IPsec tunnel defined by this rule.' and contains three sections: 1. 'Which computers are in Endpoint 1?' with a text box containing '172.31.0.0/16' and buttons for 'Add...', 'Edit...', and 'Remove'. 2. 'What is the local tunnel endpoint (closest to computers in Endpoint 1)?' with fields for 'IPv4 address:' (containing '172.31.13.36') and 'IPv6 address:', an 'Edit...' button, and a checkbox for 'Apply IPsec tunnel authorization as specified on the IPsec Settings tab of Windows Firewall with Advanced Security Properties'. 3. 'What is the remote tunnel endpoint (closest to computers in Endpoint 2)?' with fields for 'IPv4 address:' (containing '54.240.204.89') and 'IPv6 address:', an 'Edit...' button, and another 'Which computers are in Endpoint 2?' section with a text box containing '10.0.0.0/16' and an 'Add...' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

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 la sección de `IPsec tunelización`, elija `Personalizar`. Compruebe la siguiente configuración de `IPsec tunelización` y, a continuación, pulse `Aceptar` y volver a pulsar `Aceptar` para cerrar el cuadro de diálogo.
 - Está seleccionada la opción `Utilizar IPsec tunelización`.
 - El punto de enlace del túnel local (más cercano al punto de enlace 1) contiene la dirección IP del servidor de Windows. Si 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. Repita el paso 2 para el segundo túnel. Esta vez, sustituya `rule_name` por el nombre que asignó a la segunda regla de conexión.

Configurar el firewall de Windows

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

Para configurar el firewall de Windows

1. Abra el administrador del servidor, elija Tools (Herramientas), seleccione Windows Defender Firewall with Advanced Security (Firewall de Windows Defender con seguridad avanzada)y, a continuación, elija Properties (Propiedades).
2. En la pestaña IPsec Configuración, en la sección de IPsecexenciones, compruebe que Exentar ICMP de IPsec es No (opción predeterminada). Compruebe que la autorización IPsec del túnel sea Ninguna.
3. En IPsec los valores predeterminados, elija Personalizar.
4. En Intercambio de claves (modo principal), seleccione Avanzado y, a continuación, elija Personalizar.
5. En Personalizar configuración avanzada de intercambio de claves, en Métodos de seguridad, asegúrese de que se utilizan los siguientes valores predeterminados para la primera entrada:
 - Integridad: SHA-1
 - Cifrado: AES-CBC 128
 - Algoritmo de intercambio de claves: Grupo Diffie-Hellman 2
 - En Duración de la clave, asegúrese de que Minutos tenga el valor 480 y de que Sesiones tenga el valor 0.

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

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

6. En Opciones de intercambio de claves, seleccione Usar Diffie-Hellman para mayor seguridad y, a continuación, elija Aceptar.
7. En Protección de datos (modo rápido), seleccione Avanzado y, a continuación, elija Personalizar.
8. Seleccione Requerir cifrado para todas las reglas de seguridad de conexión que usan esta configuración.
9. En Integridad y cifrado de datos, deje los valores predeterminados:
 - Protocolo: ESP
 - Integridad: SHA-1
 - Cifrado: AES-CBC 128
 - Vigencia: 60 minutos

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

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

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

Paso 5: Habilitar la detección de gateways inactivas

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

Para habilitar la detección de gateways inactivas

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

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

Para obtener más información, consulte [EnableDeadGWDetect](#) en la TechNetBiblioteca de Microsoft.

Paso 6: Comprobar la conexión de VPN

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

Si desea ver los pasos para probar la conexión de VPN, consulte [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 su servidor de Windows es una instancia EC2, asegúrese de que las reglas de salida de su grupo de seguridad permitan IPsec el tráfico. Para obtener más información, consulte [Configuración de instancias de Windows](#).
- Asegúrese de que el sistema operativo de la instancia en la que está haciendo ping esté configurado para responder a ICMP. Le recomendamos que utilice uno de los sistemas Amazon Linux AMIs.
- Si la instancia a la que está haciendo ping es una instancia de Windows, conéctese a la instancia y habilite la entrada ICMPv4 en el firewall de Windows.
- Asegúrese de haber configurado las tablas de ruteo correctamente para su VPC o su subred. Para obtener más información, consulte [Paso 1: Crear una conexión de VPN y configurar la VPC](#).
- Si el dispositivo de puerta de enlace del cliente es una instancia EC2, asegúrese de haber desactivado la source/destination comprobación 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.

Resolución de problemas AWS Site-to-Site VPN Dispositivo de gateway de cliente

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

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

Temas

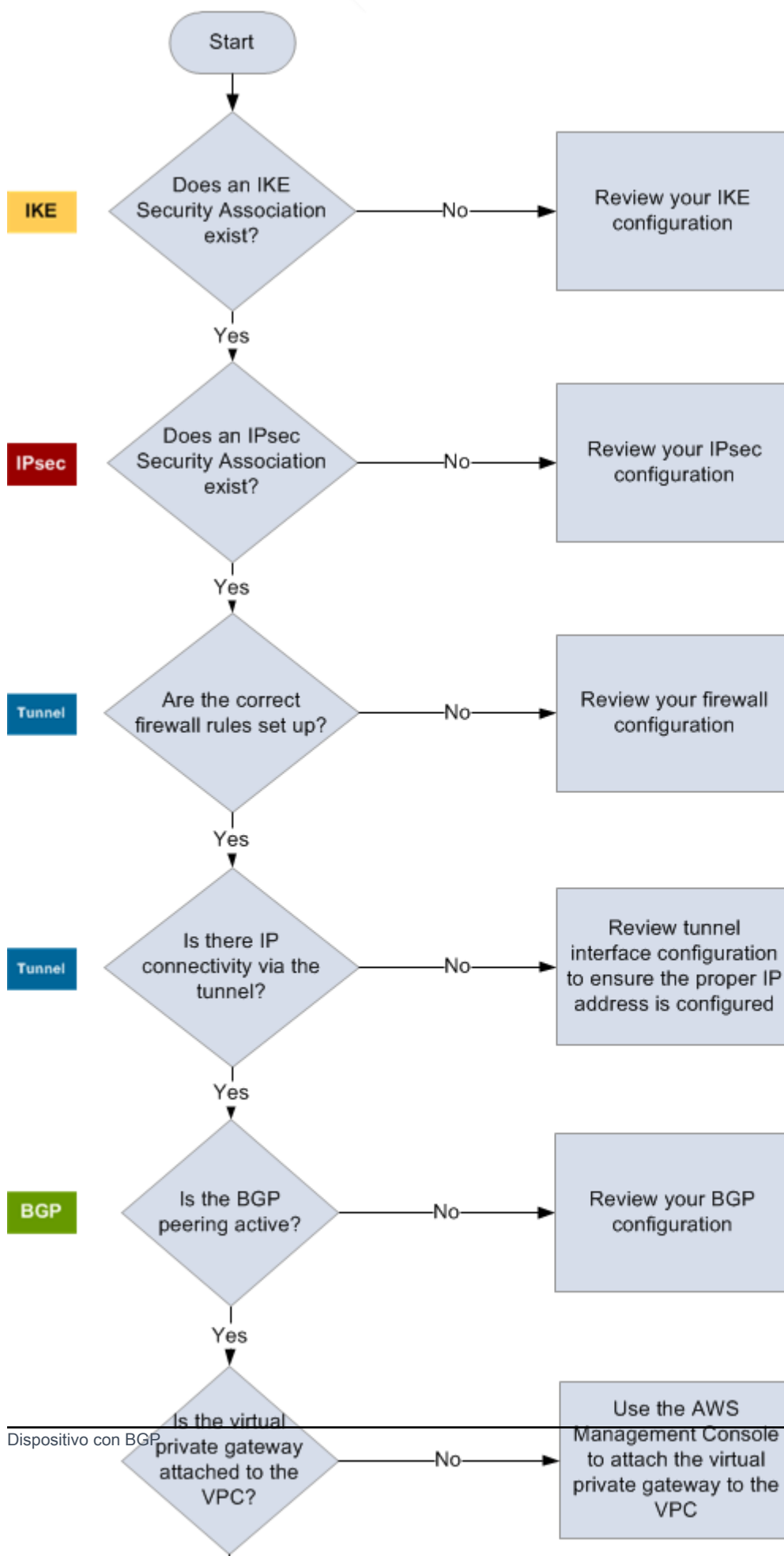
- [Solución de problemas AWS Site-to-Site VPN conectividad cuando se utiliza el protocolo Border Gateway](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad sin el protocolo Border Gateway](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco ASA](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS sin el protocolo Border Gateway](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de pasarela de clientes JunOS de Juniper](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Juniper ScreenOS](#)
- [Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de pasarela de clientes de Yamaha](#)

Recursos adicionales

- [Foro de Amazon VPC](#)

Solución de problemas AWS Site-to-Site VPN conectividad cuando se utiliza el protocolo Border Gateway

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

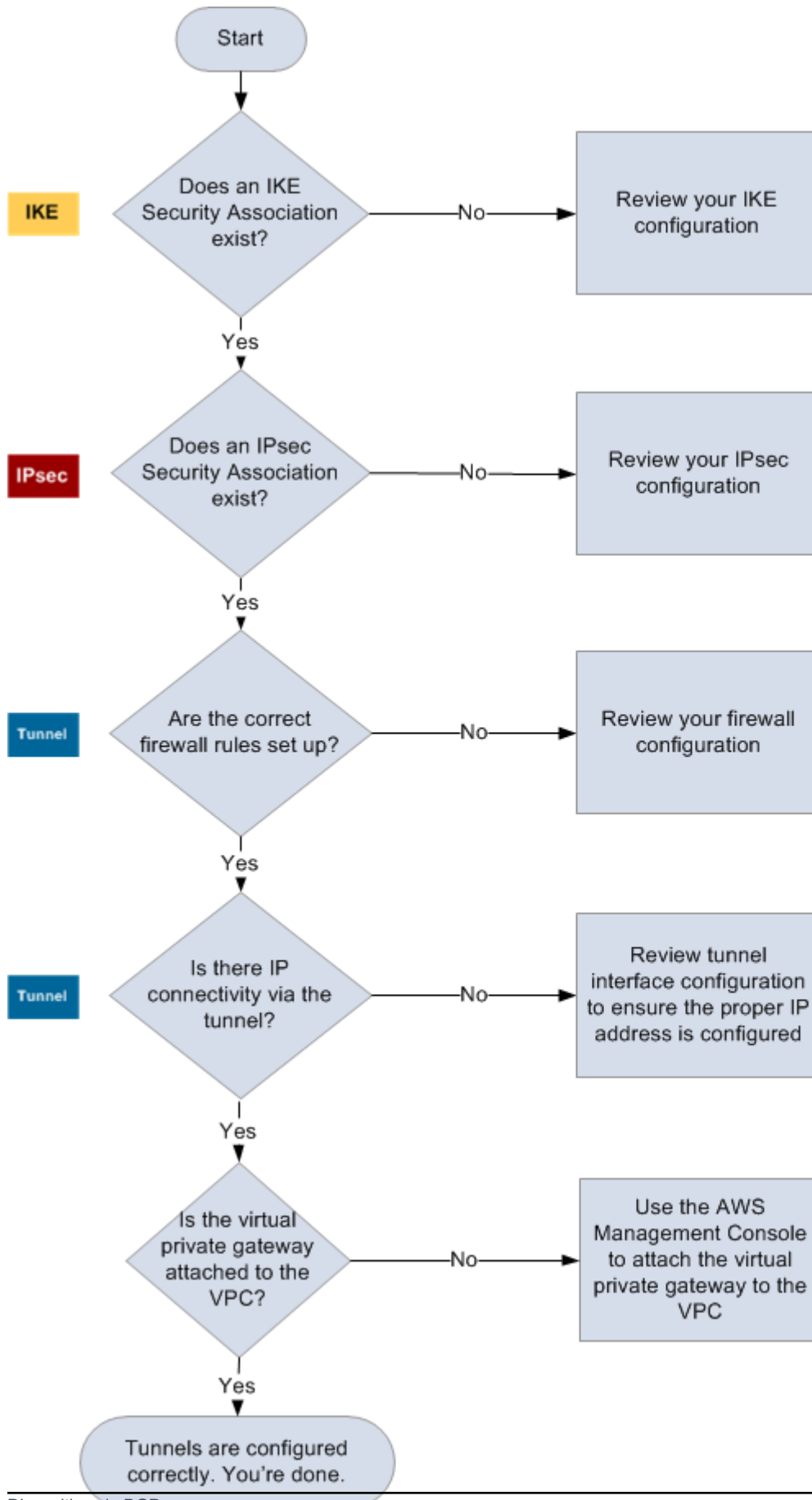


IKE	Determine si existe una asociación de seguridad de IKE. Es necesario tener una asociación de seguridad de IKE para intercambiar las claves que se utilizan para establecer la asociación de seguridad de IPsec. Si no existe ninguna asociación de seguridad de IKE, revise sus opciones de configuración 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 AWS Site-to-Site VPN Dispositivo de gateway de cliente). Si están correctamente configuradas, continúe. Determine si hay conectividad IP a través del túnel. Cada lado del túnel tiene una dirección IP según lo especificado en el archivo de configuración. La dirección de gateway privada virtual es la dirección utilizada como la dirección vecina de BGP. Desde su dispositivo de gateway de cliente, haga ping a esta dirección para determinar si el tráfico IP se está cifrando y descifrando correctamente. Si el ping no se realiza correctamente, revise la configuración de la interfaz del túnel para asegurarse de que se ha configurado la dirección IP adecuada. Si el ping es correcto, vaya a “BGP”.

BGP	Determine si la sesión de intercambio de tráfico BGP está activa. Para cada túnel, haga lo siguiente: • En su dispositivo de gateway de cliente, determine si el estado de BGP es <code>Active</code> o <code>Established</code> . El intercambio de tráfico BGP puede tardar aproximadamente 30 segundos en activarse. • Asegúrese de que el dispositivo de puerta de enlace del cliente anuncie la ruta predeterminada (0.0.0. 0/0) a la puerta de enlace 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 AWS Site-to-Site VPN conectividad sin el protocolo Border Gateway

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



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 AWS Site-to-Site VPN Dispositivo de gateway de cliente). Si están correctamente configuradas, continúe. Determine si hay conectividad IP a través del túnel. Cada lado del túnel tiene una dirección IP según lo especificado en el archivo de configuración. La dirección de gateway privada virtual es la dirección utilizada como la dirección vecina de BGP. Desde su dispositivo de gateway de cliente, haga ping a esta dirección para determinar si el tráfico IP se está cifrando y descifrando correctamente. Si el ping no se realiza correctamente, revise la configuración de la interfaz del túnel para asegurarse de que se ha configurado la dirección IP adecuada. Si el ping se realiza correctamente, vaya a “Rutas estáticas”.

**Rutas
estáticas**

Para cada túnel, haga lo siguiente:

- Compruebe que ha añadido una ruta estática a su CIDR de VPC con los túneles como el siguiente salto.
- Asegúrese de que ha agregado una ruta estática en la consola de Amazon VPC para indicar a la gateway privada virtual que dirija 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 AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes 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 ASA de Cisco solo admiten Active/Standby el modo. 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. El siguiente ejemplo de lista de acceso permite que todo el tráfico interno vaya a la subred 10.0.0 de la VPC. 0/16.

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

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

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

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

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 AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes 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 AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

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

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.255.2/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 72.21.209.225
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

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

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

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

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

Debería ver cinco signos de exclamación.

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

BGP

Use el siguiente comando.

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

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

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

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

Si la interconexión BGP está activa, compruebe que el dispositivo de puerta de enlace del cliente anuncie 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 AWS Site-to-Site VPN conectividad con un dispositivo de puerta de enlace para clientes Cisco IOS sin el protocolo Border Gateway

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 pcg 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 pcg 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 AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

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

```
router# show interfaces tun1
```

```
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 169.254.249.18/30
  MTU 17867 bytes, BW 100 Kbit/sec, DLY 50000 usec,
    reliability 255/255, txload 2/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 174.78.144.73, destination 205.251.233.121
  Tunnel protocol/transport IPSEC/IP
  Tunnel TTL 255
  Tunnel transport MTU 1427 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "ipsec-vpn-92df3bfb-0")
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 1 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
    407 packets input, 30010 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
```

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

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

```
router# ping 169.254.249.18 df-bit size 1410
```

```
Type escape sequence to abort.  
Sending 5, 1410-byte ICMP Echos to 169.254.249.18, timeout is 2 seconds:  
Packet sent with the DF bit set  
!!!!!!
```

Debería ver cinco signos de exclamación.

Enrutamiento

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

```
router# sh ip route static
```

```
1.0.0.0/8 is variably subnetted  
S      10.0.0.0/16 is directly connected, Tunnel1  
is directly connected, Tunnel2
```

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

```
router# ip route 10.0.0.0 255.255.0.0 Tunnel1 track 100  
router# ip route 10.0.0.0 255.255.0.0 Tunnel2 track 200
```

Comprobación de la monitorización de SLA

```
router# show ip sla statistics 100
```

```
IPSLAs Latest Operation Statistics
```

```
IPSLA operation id: 100
```

```
Latest RTT: 128 milliseconds
```

```
Latest operation start time: *18:08:02.155 UTC Wed Jul 15 2012
```

```
Latest operation return code: OK
```

```
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

```
router# show ip sla statistics 200
```

IPSLAs Latest Operation Statistics

```
IPSLA operation id: 200
    Latest RTT: 128 milliseconds
Latest operation start time: *18:08:02.155 UTC Wed Jul 15 2012
Latest operation return code: OK
Number of successes: 3
Number of failures: 0
Operation time to live: Forever
```

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

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

Solución de problemas AWS Site-to-Site VPN conectividad con un dispositivo de pasarela de clientes JunOS de Juniper

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 AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

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

```
user@router> show interfaces st0.1
```

```
Logical interface st0.1 (Index 70) (SNMP ifIndex 126)
  Flags: Point-To-Point SNMP-Traps Encapsulation: Secure-Tunnel
  Input packets : 8719
  Output packets: 41841
  Security: Zone: Trust
  Allowed host-inbound traffic : bgp ping ssh traceroute
  Protocol inet, MTU: 9192
    Flags: None
    Addresses, Flags: Is-Preferred Is-Primary
    Destination: 169.254.255.0/30, Local: 169.254.255.2
```

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

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

```
user@router> ping 169.254.255.1 size 1382 do-not-fragment
```

```
PING 169.254.255.1 (169.254.255.1): 1410 data bytes
64 bytes from 169.254.255.1: icmp_seq=0 ttl=64 time=71.080 ms
64 bytes from 169.254.255.1: icmp_seq=1 ttl=64 time=70.585 ms
```

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

BGP

Ejecute el comando siguiente.

```
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 la interconexión BGP está activa, compruebe que el dispositivo de puerta de enlace del cliente anuncie 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              0

```

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

```

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

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

IKE 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 AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

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

```
ssg5-serial-> get interface tunnel.1
```

```
Interface tunnel.1:
description tunnel.1
number 20, if_info 1768, if_index 1, mode route
link ready
vsys Root, zone Trust, vr trust-vr
admin mtu 1500, operating mtu 1500, default mtu 1500
*ip 169.254.255.2/30
*manage ip 169.254.255.2
route-deny disable
bound vpn:
    IPSEC-1

Next-Hop Tunnel Binding table
Flag Status Next-Hop(IP)    tunnel-id  VPN

pmtu-v4 disabled
ping disabled, telnet disabled, SSH disabled, SNMP disabled
web disabled, ident-reset disabled, SSL disabled

OSPF disabled  BGP enabled  RIP disabled  RIPng disabled  mtrace disabled
PIM: not configured  IGMP not configured
NHRP disabled
bandwidth: physical 0kbps, configured egress [gbw 0kbps mbw 0kbps]
            configured ingress mbw 0kbps, current bw 0kbps
            total allocated gbw 0kbps
```

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

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

```
ssg5-serial-> ping 169.254.255.1
```

```
Type escape sequence to abort
```

```
Sending 5, 100-byte ICMP Echos to 169.254.255.1, timeout is 1 seconds
!!!!!!
```

Success Rate is 100 percent (5/5), round-trip time min/avg/max=32/32/33 ms

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

BGP

Ejecute el comando siguiente.

```
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 la interconexión BGP está activa, compruebe que su dispositivo de pasarela de clientes anuncie 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 AWS Site-to-Site VPN conectividad con un dispositivo de pasarela de clientes 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 al conectarse a la Site-to-Site VPN. Si no proxy ID está configurado en su router, consulte el ejemplo de archivo AWS de configuración proporcionado para que Yamaha lo configure correctamente.

IKE

Ejecute el comando siguiente. 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 comando siguiente. 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 AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

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

```
# show status tunnel 1
```

```
TUNNEL[1]:
Description:
  Interface type: IPsec
  Current status is Online.
  from 2011/08/15 18:19:45.
  5 hours 7 minutes 58 seconds connection.
Received:      (IPv4) 3933 packets [244941 octets]
               (IPv6) 0 packet [0 octet]
Transmitted:   (IPv4) 3933 packets [241407 octets]
               (IPv6) 0 packet [0 octet]
```

Asegúrese de que el 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 comando siguiente.

```
# 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 la interconexión BGP está activa, compruebe que su dispositivo de pasarela de clientes anuncie 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

Integración de AWS Site-to-Site VPN y eero

AWS Site-to-Site VPN ha colaborado con [eero](#) para que las organizaciones puedan establecer una conectividad segura entre sus sitios remotos y AWS de forma sencilla y cómoda con tan solo unos clics.

Esta solución aprovecha los puntos de WiFi acceso y las pasarelas de red de eero para proporcionar conectividad local. Con los dispositivos de puerta de enlace y la Site-to-Site VPN de eero, los clientes pueden establecer automáticamente la conectividad VPN para acceder a sus aplicaciones alojadas en AWS, como las pasarelas de pago para los sistemas de punto de venta, con solo unos pocos clics. Esto facilita y agiliza a los clientes la tarea de ampliar la conectividad de sus sitios remotos a cientos de sitios y elimina la necesidad de contar con un técnico in situ con experiencia en redes para configurar la conectividad. Esta solución es adecuada para empresas distribuidas con hasta 500 oficinas remotas, y cada oficina tiene hasta 100 usuarios.

Para obtener más información sobre esta integración, incluida una guía de configuración detallada, consulte la documentación de [eero](#).

Note

No hay cambios en la funcionalidad de AWS Site-to-Site VPN como parte de esta integración.

Consideraciones:

- Disponible solo para conexiones VPN conectadas a una Transit Gateway o a una WAN en la nube. No es compatible con los archivos adjuntos de una puerta de enlace privada virtual.
- No se admiten túneles de 5 Gbps.

- Site-to-Site No se admite el concentrador VPN.
- Site-to-Site [Las cuotas](#) de VPN no cambian con esta integración.

Trabaja con AWS Site-to-Site VPN

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

Temas

- [Creación y administración de AWS Site-to-Site VPN concentradores](#)
- [Crear una AWS Site-to-Site VPN conexión](#)
- [Prueba de una conexión de AWS Site-to-Site VPN](#)
- [Eliminación de una conexión de AWS Site-to-Site VPN y una puerta de enlace](#)
- [Modificar la puerta de enlace de destino de una AWS Site-to-Site VPN conexión](#)
- [Modificar AWS Site-to-Site VPN opciones de conexión](#)
- [Modificar opciones de túnel de AWS Site-to-Site VPN](#)
- [Edición de rutas estáticas para una conexión de AWS Site-to-Site VPN](#)
- [Cambio de la puerta de enlace de cliente para una conexión de AWS Site-to-Site VPN](#)
- [Sustitución de las credenciales comprometidas por una conexión de AWS Site-to-Site VPN](#)
- [Rotación de certificados de punto de conexión de túnel de AWS Site-to-Site VPN](#)
- [IP privada AWS Site-to-Site VPN con Direct Connect](#)

Creación y administración de AWS Site-to-Site VPN concentradores

Los concentradores VPN le permiten agregar y administrar múltiples conexiones VPN desde sitios remotos, lo que proporciona una administración centralizada.

Tras crear los concentradores de Site-to-Site VPN, podrá verlos y gestionarlos desde la página principal de los concentradores de Site-to-Site VPN de la consola de Amazon VPC. Este panel muestra todos los concentradores de VPN activos que gestionan las conexiones seguras entre AWS y sus sitios remotos.

Temas

- [Crear un AWS Site-to-Site VPN concentrador](#)
- [Administrar etiquetas de AWS Site-to-Site VPN Concentrador](#)
- [Eliminar un AWS Site-to-Site VPN concentrador](#)

Crear un AWS Site-to-Site VPN concentrador

Cree un concentrador mediante la consola Amazon VPC, APIs la o la. AWS CLI Antes de crear un concentrador, primero debe haber creado una puerta de enlace de tránsito para asociarla al concentrador. Para obtener más información sobre la creación de pasarelas de tránsito, consulte [Crear una pasarela de tránsito](#) en la Guía de pasarelas de tránsito de Amazon AWS VPC.

Cree un concentrador de Site-to-Site VPN mediante la consola

Para crear un concentrador Site-to-Site VPN mediante la consola AWS de administración, siga estos pasos:

Para crear un concentrador Site-to-Site VPN mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Site-to-Site Concentradores VPN.
3. Elija Crear concentrador de Site-to-Site VPN.
4. (Opcional) En la etiqueta con el nombre, introduzca un nombre para su concentrador de Site-to-Site VPN.
5. Para Transit Gateway, selecciona una pasarela de tránsito existente.
6. (Opcional) Agregue etiquetas para ayudar a identificar y organizar su concentrador de Site-to-Site VPN.
 - a. Elija Añadir nueva etiqueta.
 - b. En Key, introduzca una clave de etiqueta (por ejemplo, **Name**).
 - c. En Valor, introduzca un valor de etiqueta (por ejemplo, **Production-VPN-Concentrator**).
 - d. Repita los pasos anteriores para añadir etiquetas adicionales según sea necesario.
7. Elija Crear concentrador de Site-to-Site VPN.

Tras su creación, el concentrador Site-to-Site VPN estará en ese pending estado mientras se aprovisiona. Cuando esté listo, el estado cambiará a available y podrás empezar a crear conexiones VPN que usen el concentrador Site-to-Site VPN.

Cree un concentrador Site-to-Site VPN mediante la CLI

Antes de crear un concentrador Site-to-Site VPN mediante la CLI, asegúrese de tener lo siguiente:

- Un Transit Gateway existente en tu AWS cuenta
- Permisos de IAM adecuados para crear concentradores de Site-to-Site VPN
- El ID de la Transit Gateway a la que quieres conectar el Concentrador

El siguiente ejemplo crea un concentrador de Site-to-Site VPN para la puerta de enlace de tránsito especificada:

```
aws ec2 create-vpn-concentrator --transit-gateway-id tgw-123456789
```

A continuación se muestra una respuesta correcta:

```
{
  "VpnConcentrator": {
    "VpnConcentratorId": "vcn-0123456789abcdef0",
    "State": "pending",
    "TransitGatewayId": "tgw-123456789",
    "CreationTime": "2025-09-29T17:26:31.000Z",
    "Tags": []
  }
}
```

Cree un concentrador de Site-to-Site VPN mediante la API

Puede crear un concentrador de Site-to-Site VPN mediante la `CreateVpnConcentrators` API.

La API acepta los siguientes parámetros clave:

`TransitGatewayId`

El ID de la Transit Gateway a la que se va a conectar el concentrador Site-to-Site VPN.

`TagSpecification`

Etiquetas que se van a asignar al concentrador de Site-to-Site VPN para la organización y facturación de los recursos.

El siguiente ejemplo muestra cómo crear un concentrador Site-to-Site VPN conectado a una Transit Gateway:

```
POST / HTTP/1.1
```

```
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=...

Action=CreateVpnConcentrator
&Version=2016-11-15
&TransitGatewayId=tgw-0123456789abcdef0
&TagSpecification.1.ResourceType=vpn-concentrator
&TagSpecification.1.Tag.1.Key=Name
&TagSpecification.1.Tag.1.Value=MyVpnConcentrator
```

Tras la creación correcta, la API devuelve detalles sobre el concentrador Site-to-Site VPN recién creado:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConcentratorResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>12345678-1234-1234-1234-123456789012</requestId>
  <vpnConcentrator>
    <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
    <state>pending</state>
    <transitGatewayId>tgw-0123456789abcdef0</transitGatewayId>
    <creationTime>2024-01-15T10:30:00.000Z</creationTime>
    <tagSet>
      <item>
        <key>Name</key>
        <value>MyVpnConcentrator</value>
      </item>
    </tagSet>
  </vpnConcentrator>
</CreateVpnConcentratorResponse>
```

Administrar etiquetas de AWS Site-to-Site VPN Concentrator

Las etiquetas son pares clave-valor que le ayudan a organizar y administrar sus concentradores de Site-to-Site VPN. Puede utilizar etiquetas para clasificar los concentradores de Site-to-Site VPN por finalidad, entorno, centro de costes o cualquier otro criterio que tenga sentido para su organización.

Administre las etiquetas mediante la consola

Puede añadir o eliminar etiquetas para un concentrador Site-to-Site VPN mediante la consola AWS de administración.

Para añadir etiquetas a un concentrador 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 Concentradores VPN.
3. Seleccione el concentrador Site-to-Site VPN que desee etiquetar.
4. Elija la pestaña Etiquetas.
5. Elija Manage tags (Administrar etiquetas).
6. Elija Add new tag (Agregar nueva etiqueta).
7. En Clave, introduzca una clave de etiqueta (por ejemplo, **Environment**).
8. En Valor, introduzca un valor de etiqueta (por ejemplo, **Production**).
9. Seleccione Save changes (Guardar cambios).

Para eliminar etiquetas de un Site-to-Site concentrador 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 Concentradores VPN.
3. Seleccione el concentrador Site-to-Site VPN del que desee eliminar las etiquetas.
4. Elija la pestaña Etiquetas.
5. Elija Administrar etiquetas.
6. Para cada etiqueta que desee eliminar, seleccione Eliminar.
7. Seleccione Save changes (Guardar cambios).

Administre las etiquetas mediante la CLI

Puede añadir, modificar o eliminar etiquetas mediante AWS CLI.

Agregar etiquetas.

El siguiente ejemplo agrega etiquetas a un concentrador Site-to-Site VPN:

```
aws ec2 create-tags --resources vcn-0123456789abcdef0 --tags  
Key=Environment,Value=Production Key=Team,Value=NetworkOps
```

En caso de éxito, este comando no devuelve ningún resultado.

Consulta de etiquetas

El siguiente ejemplo describe las etiquetas de un concentrador Site-to-Site VPN:

```
aws ec2 describe-tags --filters "Name=resource-id,Values=vcn-0123456789abcdef0"
```

Se devuelve la siguiente respuesta:

```
{
  "Tags": [
    {
      "Key": "Environment",
      "ResourceId": "vcn-0123456789abcdef0",
      "ResourceType": "vpn-concentrator",
      "Value": "Production"
    },
    {
      "Key": "Team",
      "ResourceId": "vcn-0123456789abcdef0",
      "ResourceType": "vpn-concentrator",
      "Value": "NetworkOps"
    }
  ]
}
```

Eliminación de etiquetas

El siguiente ejemplo elimina las etiquetas de un Site-to-Site concentrador VPN:

```
aws ec2 delete-tags --resources vcn-0123456789abcdef0 --tags Key=Environment Key=Team
```

En caso de éxito, este comando no devuelve ningún resultado.

Gestione las etiquetas mediante la API

Puede gestionar mediante programación las etiquetas de Site-to-Site VPN Concentrator mediante las operaciones de la API de Amazon EC2 .

CreateTags

Utilice la CreateTags operación para añadir o actualizar etiquetas:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
```

```
Content-Type: application/x-www-form-urlencoded
```

```
Action=CreateTags
&ResourceId.1=vcn-0123456789abcdef0
&Tag.1.Key=Environment
&Tag.1.Value=Production
&Tag.2.Key=Team
&Tag.2.Value=NetworkOps
&Version=2016-11-15
```

Se devuelve la siguiente respuesta:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
  <return>true</return>
</CreateTagsResponse>
```

DescribeTags

Utilice la DescribeTags operación para recuperar etiquetas:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DescribeTags
&Filter.1.Name=resource-id
&Filter.1.Value.1=vcn-0123456789abcdef0
&Version=2016-11-15
```

Se devuelve la siguiente respuesta:

```
<?xml version="1.0" encoding="UTF-8"?>
<DescribeTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
  <tagSet>
    <item>
      <resourceId>vcn-0123456789abcdef0</resourceId>
      <resourceType>vpn-concentrator</resourceType>
      <key>Environment</key>
      <value>Production</value>
    </item>
  </tagSet>
</DescribeTagsResponse>
```

```
<item>
  <resourceId>vcn-0123456789abcdef0</resourceId>
  <resourceType>vpn-concentrator</resourceType>
  <key>Team</key>
  <value>NetworkOps</value>
</item>
</tagSet>
</DescribeTagsResponse>
```

DeleteTags

Utilice la DeleteTags operación para eliminar etiquetas:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DeleteTags
&ResourceId.1=vcn-0123456789abcdef0
&Tag.1.Key=Environment
&Tag.2.Key=Team
&Version=2016-11-15
```

Se devuelve la siguiente respuesta:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteTagsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
  <return>true</return>
</DeleteTagsResponse>
```

Eliminar un AWS Site-to-Site VPN concentrador

Cuando ya no necesite un concentrador Site-to-Site VPN, puede eliminarlo para dejar de incurrir en cargos. Al eliminar un concentrador Site-to-Site VPN, se elimina de forma permanente este y todas las configuraciones asociadas.

Requisitos previos

Antes de eliminar un concentrador Site-to-Site VPN, asegúrese de lo siguiente:

- Se eliminan todas las conexiones Site-to-Site VPN asociadas al concentrador VPN.

- Dispone de los permisos necesarios para eliminar los concentradores Site-to-Site VPN (`ec2:DeleteVpnConcentrator`).

Elimine un concentrador Site-to-Site VPN mediante la consola

Para eliminar un concentrador 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 Concentradores de sitio a sitio.
3. Seleccione el concentrador de Site-to-Site VPN que desee eliminar.
4. Elija Acciones y, a continuación, elija Eliminar el concentrador de Site-to-Site VPN.
5. En el cuadro de diálogo de confirmación, ingrese **delete** para confirmar la eliminación.
6. Elija Eliminar.

Eliminar un concentrador Site-to-Site VPN mediante la CLI

Utilice el `delete-vpn-concentrator` comando para eliminar un concentrador Site-to-Site VPN. Necesitarás `vpn-concentrator-id` el para eliminarlo.

El siguiente ejemplo elimina un concentrador de Site-to-Site VPN:

```
aws ec2 delete-vpn-concentrator --vpn-concentrator-id vcn-0123456789abcdef0
```

Se devuelve la siguiente respuesta:

```
{
  "VpnConcentrator": {
    "VpnConcentratorId": "vcn-0123456789abcdef0",
    "State": "deleting",
    "Message": "The Site-to-Site VPN Concentrator vcn-0123456789abcdef0 is being
deleted and will be removed from your account."
  }
}
```

Elimine un concentrador de Site-to-Site VPN mediante la API

Utilice la `DeleteVpnConcentrator` operación para eliminar un concentrador Site-to-Site VPN. Necesitarás `VpnConcentratorId` el para eliminarlo.

El siguiente ejemplo elimina un concentrador de Site-to-Site VPN:

```
POST / HTTP/1.1
Host: ec2.region.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=DeleteVpnConcentrator
&VpnConcentratorId=vcn-0123456789abcdef0
&Version=2016-11-15
```

Se devuelve la siguiente respuesta:

```
<?xml version="1.0" encoding="UTF-8"?>
<DeleteVpnConcentratorResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
  <vpnConcentrator>
    <vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
    <state>deleting</state>
    <message>The Site-to-Site VPN Concentrator vcn-0123456789abcdef0 is being
deleted and will be removed from your account.</message>
  </vpnConcentrator>
</DeleteVpnConcentratorResponse>
```

Crear una AWS Site-to-Site VPN conexión

Puedes crear conexiones Site-to-Site VPN que se conecten a pasarelas de tránsito o a redes globales de Cloud WAN. Ambos tipos de adjuntos admiten IPv6 protocolos IPv4 y, si lo desea, puede utilizar concentradores Site-to-Site VPN para conectar varios sitios remotos de forma rentable.

Cree una conexión VPN mediante la consola

Para crear una conexión VPN mediante la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. (Opcional) En Etiqueta de nombre, escriba el nombre de la conexión. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.

5. En el tipo de puerta de enlace de destino, elija una de las siguientes opciones:
 - Puerta de enlace privada virtual: cree una nueva conexión VPN de puerta de enlace privada virtual eligiendo una puerta de enlace privada virtual existente.
 - Puerta de enlace de tránsito: cree una nueva conexión VPN de puerta de enlace de tránsito eligiendo una puerta de enlace de tránsito existente. Para obtener más información acerca de cómo crear una gateway de tránsito, consulte [Gateways de tránsito](#) en Gateways de tránsito de Amazon VPC.
 - Site-to-Site Concentrador VPN: cree una nueva conexión de concentrador Site-to-Site VPN utilizando un concentrador Site-to-Site VPN existente o creando uno nuevo. Seleccione una de las siguientes opciones:
 - Existente: cree una nueva conexión Site-to-Site VPN con un concentrador VPN utilizando un concentrador existente.
 - Nuevo: introduzca un nombre opcional para el concentrador Site-to-Site VPN y, a continuación, elija la pasarela de tránsito para asociarlo.
 - No asociada: crea una conexión VPN independiente que luego se pueda asociar a Cloud WAN a través de la consola o la API de Network Manager. Para obtener más información sobre los adjuntos de VPN y Cloud WAN, consulta los [adjuntos de Site-to-site VPN en AWS Cloud WAN](#) en la Guía del usuario de AWS Cloud WAN.
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 pasarela de clientes, selecciona Nueva y, a continuación, haz lo siguiente:
 - Para la dirección IP, introduzca una IPv6dirección estática IPv4o.
 - En ARN de certificado, elija el ARN de su certificado privado (si utiliza autenticación basada en certificados).
 - 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.

 Note

Las conexiones VPN WAN en la nube y las conexiones VPN que utilizan concentradores solo admiten el enrutamiento BGP. El enrutamiento estático no es compatible con estos tipos de conexión.

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. Para la versión Tunnel inside IP, elija IPv4o 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 de .

11. (Opcional) Según qué túnel de la versión de IP haya elegido, realice una de las siguientes operaciones:
 - IPv4 — Para el CIDR de IPv4 red local, especifique el rango de IPv4 CIDR en la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles de la VPN. Para el CIDR IPv4 de red remota, elija el rango de CIDR en el AWS lado que puede comunicarse a través de los túneles de la VPN. El valor predeterminado de ambos campos es 0.0.0.0/0.
 - IPv6 — Para el CIDR de IPv6 red local, especifique el rango de IPv6 CIDR en la puerta de enlace del cliente (local) que puede comunicarse a través de los túneles VPN. Para el CIDR IPv6 de red remota, elija el rango de CIDR en el AWS lado que puede comunicarse a través de los túneles de la VPN. El valor predeterminado de ambos campos es ::/0
12. En Tipo de dirección IP externa, elija una de las siguientes opciones:
 - Público IPv4: (predeterminado) Usa IPv4 direcciones para el túnel exterior. IPs
 - Privado IPv4: utilice una IPv4 dirección privada para utilizarla en redes privadas.
 - IPv6- Usa IPv6 las direcciones del túnel exterior IPs. Esta opción requiere que el dispositivo de pasarela de clientes sea compatible con el IPv6 direccionamiento.

 Note

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

13. (Opcional) En Opciones de túnel 1, puede especificar la siguiente información para cada túnel:
 - Un bloque IPv4 CIDR de tamaño /30 del 169.254.0.0/16 rango de las direcciones del túnel IPv4 interior.
 - Si especificó IPv6 para la versión Tunnel inside IP, un bloque IPv6 CIDR /126 del fd00::/8 rango para las direcciones del túnel interno. IPv6
 - La clave previamente compartida de IKE (PSK). Se admiten las siguientes versiones: IKEv1 o IKEv2
 - Para editar las opciones avanzadas del túnel, seleccione Editar opciones de túnel. Para obtener más información, consulte [Opciones de túnel de VPN](#).
 - (Opcional) Seleccione Activar en el registro de actividad del túnel para capturar los mensajes de registro de IPsec la actividad y los mensajes del protocolo DPD.
 - (Opcional) Seleccione Activar para 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).

Cree una conexión de pasarela de AWS Site-to-Site VPN tránsito mediante la CLI o la API

Cree una conexión VPN a Transit Gateway mediante la CLI

Usa el [create-vpn-connection](#) comando y especifica el ID de la pasarela de tránsito para la -- transit-gateway-id opción.

El siguiente ejemplo muestra la creación de una conexión VPN con un túnel IPv6 exterior IPs y un túnel IPv6 interior IPs:

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

Ejemplo de respuesta:

```
{
  "VpnConnection": {
    "VpnConnectionId": "vpn-0abcdef1234567890",
    "State": "pending",
    "CustomerGatewayId": "cgw-001122334455aabbcc",
    "Type": "ipsec.1",
    "TransitGatewayId": "tgw-12312312312312312",
    "Category": "VPN",
    "Routes": [],
    "Options": {
      "StaticRoutesOnly": false,
      "OutsideIPAddressType": "Ipv6",
      "TunnelInsideIpVersion": "ipv6"
    }
  }
}
```

Cree una conexión VPN a Transit Gateway mediante la API

Puede crear una conexión VPN mediante la API de Amazon EC2. En esta sección se proporcionan ejemplos de mensajes de solicitud y respuesta para crear una conexión VPN de Transit Gateway mediante la API.

Requisitos previos

Antes de crear una conexión VPN mediante la API, asegúrate de tener:

- Se ha creado y está disponible una pasarela de tránsito

- Una pasarela de clientes configurada con los detalles de su dispositivo local

En el siguiente ejemplo, se muestra cómo crear una conexión VPN mediante la acción de la `CreateVpnConnection` API:

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=CreateVpnConnection
&Type=ipsec.1
&TransitGatewayId=tgw-12345678901234567
&CustomerGatewayId=cgw-12345678901234567
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

En este ejemplo, se crea una conexión VPN con enrutamiento dinámico (BGP) entre la puerta de enlace de tránsito especificada y la puerta de enlace del cliente.

Si la API responde correctamente, se muestran los detalles de la conexión VPN:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>7a62c49f-347e-4fc4-9331-6e8eEXAMPLE</requestId>
  <vpnConnection>
    <vpnConnectionId>vpn-1a2b3c4d5e6f78901</vpnConnectionId>
    <state>pending</state>
    <customerGatewayId>cgw-12345678901234567</customerGatewayId>
    <type>ipsec.1</type>
    <transitGatewayId>tgw-12345678901234567</transitGatewayId>
    <category>VPN</category>
    <options>
      <staticRoutesOnly>false</staticRoutesOnly>
    </options>
  </vpnConnection>
</CreateVpnConnectionResponse>
```

La respuesta incluye el ID de la conexión VPN, el estado actual y los detalles de configuración. La conexión estará inicialmente en estado «pendiente» mientras AWS aprovisiona los túneles de la VPN.

Crea una conexión WAN a AWS Site-to-Site VPN la nube mediante la CLI o la API

Puedes crear una conexión Site-to-Site VPN entre tu WAN local y la de AWS Cloud siguiendo el procedimiento que se indica a continuación. Para obtener más información, consulta los [archivos adjuntos de Site-to-site VPN en AWS Cloud WAN](#) en la Guía del usuario de AWS Cloud WAN.

Crea una conexión VPN a Cloud WAN mediante la CLI

Usa el [create-vpn-connection](#) comando para crear una conexión VPN que luego se conectará a una red global de Cloud WAN. Esto crea una conexión VPN independiente que, posteriormente, se puede asociar a Cloud WAN a través de la consola o la API de Network Manager.

Requisitos previos

Antes de crear una conexión VPN de Cloud WAN, asegúrate de tener lo siguiente:

- `customer-gateway-id`- Un recurso de pasarela de cliente existente (cgw-xxxxxxxxxx) que represente tu dispositivo VPN local.
- Red global WAN en la nube: se debe crear y configurar una red global WAN en la nube con los segmentos de red adecuados.
- Configuración BGP: las conexiones VPN WAN en la nube requieren el enrutamiento BGP; no se admite el enrutamiento estático. Debe configurar el `StaticRoutesOnly=false` parámetro options

Este comando crea una conexión VPN sin especificar una puerta de enlace de destino. La conexión estará desconectada y, posteriormente, se podrá asociar a tu red global de Cloud WAN a través de la consola o la API de Network Manager. La `StaticRoutesOnly=false` opción habilita el enrutamiento BGP, que es obligatorio para los archivos adjuntos a la VPN de Cloud WAN, ya que no se admite el enrutamiento estático.

En el siguiente ejemplo, se crea una conexión VPN independiente para Cloud WAN:

```
aws ec2 create-vpn-connection \
    --type ipsec.1 \
    --customer-gateway-id cgw-0123456789abcdef0 \
    --options StaticRoutesOnly=false
```

La respuesta devuelve lo siguiente:

```
{
  "VpnConnection": {
    "VpnConnectionId": "vpn-0abcdef1234567890",
    "State": "pending",
    "CustomerGatewayId": "cgw-0123456789abcdef0",
    "Type": "ipsec.1",
    "Category": "VPN",
    "Routes": [],
    "Options": {
      "StaticRoutesOnly": false
    }
  }
}
```

Tras crear la conexión VPN, puedes conectarla a tu red global de Cloud WAN mediante la consola de Network Manager o la llamada a la `create-site-to-site-vpn-attachment` API.

Crea una conexión VPN Cloud WAN mediante la API

Puede usar la API de EC2 para crear una conexión VPN para la integración de Cloud WAN. Esto implica realizar una llamada a la `CreateVpnConnection` API que cree una conexión VPN independiente, que luego se puede asociar a tu red global de Cloud WAN.

La solicitud de API crea una conexión VPN sin especificar una puerta de enlace de destino, lo que la deja en un estado desconectado que está lista para la integración de Cloud WAN. La conexión usa el enrutamiento BGP, que es obligatorio para los archivos adjuntos de la VPN de Cloud WAN.

En el siguiente ejemplo, se muestra la solicitud HTTP para crear una conexión VPN de Cloud WAN:

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=...

Action=CreateVpnConnection
&Type=ipsec.1
&CustomerGatewayId=cgw-0123456789abcdef0
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

La API devuelve una respuesta correcta que contiene los detalles de la conexión VPN. La conexión estará en un pending estado inicial mientras se AWS aprovisiona los túneles de la VPN, momento en el que el estado cambiará aavailable.

```
<?xml version="1.0" encoding="UTF-8"?>
  <CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
    <requestId>12345678-1234-1234-1234-123456789012</requestId>
    <vpnConnection>
      <vpnConnectionId>vpn-0abcdef1234567890</vpnConnectionId>
      <state>pending</state>
      <customerGatewayId>cgw-0123456789abcdef0</customerGatewayId>
      <type>ipsec.1</type>
      <category>VPN</category>
      <options>
        <staticRoutesOnly>false</staticRoutesOnly>
      </options>
      <vgwTelemetry/>
      <routes/>
    </vpnConnection>
  </CreateVpnConnectionResponse>
```

Detalles de la respuesta

La respuesta de la API proporciona la siguiente información clave:

- `vpnConnectionId`- El identificador único de tu conexión VPN (por ejemplo, `vpn-0abcdef1234567890`) que utilizarás para conectarla a Cloud WAN
- `estado`: inicialmente «pendiente», mientras que AWS aprovisiona los túneles de la VPN, luego pasa a «disponible» cuando está listo para su adjunto
- `categoría`: muestra «VPN», lo que indica que se trata de una conexión VPN no conectada adecuada para la integración con una WAN en la nube
- `staticRoutesOnly`- Configúrelo en «false» para habilitar el enrutamiento BGP, que es obligatorio para los archivos adjuntos a la VPN de Cloud WAN

Una vez que la conexión VPN alcance el estado «disponible», puedes conectarla a tu red global de Cloud WAN mediante la `CreateSiteToSiteVpnAttachment` API de Network Manager o a través de la consola de AWS.

Cree una conexión de AWS Site-to-Site VPN Concentrator mediante la CLI o la API

Cree una conexión de concentrador Site-to-Site VPN mediante la CLI

Después de crear un concentrador de Site-to-Site VPN, debe establecer conexiones VPN individuales desde sus sitios remotos al concentrador de Site-to-Site VPN. Cada sitio remoto requiere su propia conexión VPN que haga referencia al ID del Site-to-Site concentrador VPN. Esto permite que varios sitios remotos compartan la misma infraestructura de concentrador de Site-to-Site VPN y, al mismo tiempo, mantienen túneles separados y seguros para cada sitio.

Para establecer una conexión VPN mediante un concentrador de Site-to-Site VPN, especifique el concentrador de Site-to-Site VPN en lugar de la puerta de enlace de tránsito al crear la conexión de VPN. El siguiente ejemplo crea una conexión VPN mediante un concentrador Site-to-Site VPN:

```
aws ec2 create-vpn-connection \  
--type ipsec.1 \  
--customer-gateway-id cgw-123456789 \  
--vpn-concentrator-id vcn-0123456789abcdef0
```

Una respuesta correcta devuelve lo siguiente:

```
{  
  "VpnConnection": {  
    "VpnConnectionId": "vpn-0abcdef1234567890",  
    "State": "pending",  
    "CustomerGatewayId": "cgw-123456789",  
    "Type": "ipsec.1",  
    "VpnConcentratorId": "vcn-0123456789abcdef0",  
    "Category": "VPN",  
    "Routes": [],  
    "Options": {  
      "StaticRoutesOnly": false  
    }  
  }  
}
```

Cree una conexión de Site-to-Site VPN Concentrator mediante la API

Puede crear una conexión VPN que utilice un concentrador de Site-to-Site VPN mediante la API Amazon EC2. En esta sección se proporcionan ejemplos de mensajes de solicitud y respuesta para crear una conexión VPN con un concentrador Site-to-Site VPN.

Antes de crear una conexión VPN con un concentrador de Site-to-Site VPN mediante la API, asegúrese de tener:

- Se ha creado y está disponible un concentrador de Site-to-Site VPN
- Una pasarela de cliente configurada para su sitio remoto
- Configuración de red que permite IPsec el tráfico entre su sitio y AWS

El siguiente ejemplo muestra cómo crear una conexión VPN mediante un concentrador de Site-to-Site VPN con la acción de la `CreateVpnConnection` API:

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded

Action=CreateVpnConnection
&Type=ipsec.1
&VpnConcentratorId=vcn-0123456789abcdef0
&CustomerGatewayId=cgw-12345678901234567
&Options.StaticRoutesOnly=false
&Version=2016-11-15
```

En este ejemplo, se crea una conexión VPN entre el concentrador de Site-to-Site VPN especificado y la puerta de enlace del cliente. El concentrador Site-to-Site VPN actúa como punto final AWS lateral, lo que permite que varios sitios remotos se conecten a través de un concentrador centralizado.

Si la API responde correctamente, se muestran los detalles de la conexión VPN junto con la información del concentrador Site-to-Site VPN:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateVpnConnectionResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>8b73d60f-458f-5gc5-a442-7f9fEXAMPLE</requestId>
  <vpnConnection>
```

```
<vpnConnectionId>vpn-9z8y7x6w5v4u32109</vpnConnectionId>
<state>pending</state>
<customerGatewayId>cgw-12345678901234567</customerGatewayId>
<type>ipsec.1</type>
<vpnConcentratorId>vcn-0123456789abcdef0</vpnConcentratorId>
<category>VPN</category>
<options>
  <staticRoutesOnly>false</staticRoutesOnly>
</options>
</vpnConnection>
</CreateVpnConnectionResponse>
```

La respuesta incluye el ID de conexión VPN y hace referencia al ID del concentrador Site-to-Site VPN en lugar de a un ID de pasarela de tránsito. Esta conexión permite que su sitio remoto se comuniquen con otros sitios conectados al mismo concentrador Site-to-Site VPN, lo que habilita las topologías de hub-and-spoke red.

Ver AWS Site-to-Site VPN conexiones

Vea las conexiones VPN mediante la consola

Puede ver sus conexiones VPN y sus detalles mediante la consola de administración de AWS. Esto proporciona una interfaz visual para monitorear el estado de la conexión, el estado del túnel y los detalles de configuración.

Para ver las conexiones 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 Site-to-Site VPN Connections.
3. Seleccione su conexión VPN para ver información detallada, que incluye:
 - Estado y estado de la conexión
 - Detalles y estado de salud del túnel
 - Información sobre la ruta
 - Parámetros de configuración

La consola muestra información de estado en tiempo real y le permite monitorear la conectividad del túnel, ver las tablas de enrutamiento y acceder a los detalles de configuración para solucionar problemas.

Vea las conexiones VPN mediante la CLI

Utilice la AWS CLI para consultar y recuperar información detallada sobre sus conexiones de VPN mediante programación. Este método permite la automatización, la creación de scripts y la integración con las herramientas de monitoreo.

Para consultar todas las conexiones VPN de su cuenta y región de AWS actuales, ejecute el `describe-vpn-connections` comando sin parámetros. Sin embargo, si desea ver los detalles de una conexión VPN concreta, necesitará saber el identificador de la conexión VPN.

Para obtener información detallada de una conexión VPN específica, especifique el ID de conexión como parámetro. El siguiente ejemplo muestra una solicitud para ver los detalles de una conexión VPN específica.

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-1234567890abcdef0
```

La respuesta incluye información completa sobre la conexión VPN, incluidas las opciones de túnel, los detalles de enrutamiento y el estado actual.

- **State**- El estado actual de la conexión VPN
- **TunnelOptions**- Configuración y estado de cada túnel
- **OutsideIpAddress**- Las direcciones IP públicas de los túneles VPN
- **Routes**- Información de enrutamiento de la conexión

Ejemplo de extracto de respuesta que muestra los detalles clave de la conexión:

```
{
  "VpnConnections": [
    {
      "VpnConnectionId": "vpn-1234567890abcdef0",
      "State": "available",
      "CustomerGatewayId": "cgw-1234567890abcdef0",
      "Type": "ipsec.1",
      "Options": {
        "StaticRoutesOnly": false,
        "TunnelOptions": [
          {
            "OutsideIpAddress": "203.0.113.12",
            "TunnelInsideCidr": "169.254.10.0/30",
```

```

    "PreSharedKey": "example_key_1234567890abcdef0",
    "Phase1LifetimeSeconds": 28800,
    "Phase2LifetimeSeconds": 3600
  },
  {
    "OutsideIpAddress": "203.0.113.34",
    "TunnelInsideCidr": "169.254.11.0/30",
    "PreSharedKey": "example_key_0987654321fedcba0",
    "Phase1LifetimeSeconds": 28800,
    "Phase2LifetimeSeconds": 3600
  }
]
}
]
}
}

```

Vea las conexiones VPN mediante la API

Realiza llamadas directas a la API al EC2 servicio de Amazon para recuperar la información de conexión de la VPN. Este enfoque proporciona la máxima flexibilidad para aplicaciones personalizadas e integraciones programáticas.

La acción de la `DescribeVpnConnections` API consulta y devuelve información detallada sobre una o más conexiones VPN. Puede aplicar filtros por ID de conexión, estado u otros atributos para limitar los resultados.

A continuación, se muestra un ejemplo de solicitud para proporcionar detalles sobre una única conexión VPN.

```
POST / HTTP/1.1
Host: ec2.us-east-1.amazonaws.com
Content-Type: application/x-www-form-urlencoded
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20230101/us-east-1/ec2/
aws4_request, SignedHeaders=host;x-amz-date, Signature=example_signature

Action=DescribeVpnConnections
&VpnConnectionId.1=vpn-1234567890abcdef0
&Version=2016-11-15
```

La respuesta devuelve detalles sobre esa conexión VPN.

```
<?xml version="1.0" encoding="UTF-8"?>
<DescribeVpnConnectionsResponse xmlns="http://ec2.amazonaws.com/doc/2016-11-15/">
  <requestId>12345678-1234-1234-1234-123456789012</requestId>
  <vpnConnectionSet>
    <item>
      <vpnConnectionId>vpn-1234567890abcdef0</vpnConnectionId>
      <state>available</state>
      <customerGatewayId>cgw-1234567890abcdef0</customerGatewayId>
      <type>ipsec.1</type>
      <options>
        <staticRoutesOnly>false</staticRoutesOnly>
        <tunnelOptionSet>
          <item>
            <outsideIpAddress>203.0.113.12</outsideIpAddress>
            <tunnelInsideCidr>169.254.10.0/30</tunnelInsideCidr>
            <preSharedKey>example_key_1234567890abcdef0</preSharedKey>
          </item>
          <item>
            <outsideIpAddress>203.0.113.34</outsideIpAddress>
            <tunnelInsideCidr>169.254.11.0/30</tunnelInsideCidr>
            <preSharedKey>example_key_0987654321fedcba0</preSharedKey>
          </item>
        </tunnelOptionSet>
      </options>
    </item>
  </vpnConnectionSet>
</DescribeVpnConnectionsResponse>
```

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)

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

Puede modificar la puerta de enlace de destino de una AWS Site-to-Site VPN conexión. Hay disponibles las siguientes opciones de migración:

- De una gateway privada virtual existente a una gateway de tránsito
- Una gateway privada virtual existente a otra gateway privada virtual
- De una gateway de tránsito existente a otra gateway de tránsito
- De una gateway de tránsito existente a una gateway privada virtual

Después de modificar la puerta de enlace de destino, su conexión Site-to-Site VPN no estará disponible temporalmente durante un breve período mientras aprovisionamos los nuevos puntos de conexión.

Las siguientes tareas le ayudan a realizar la migración a una nueva gateway.

Tareas

- [Paso 1: Crear la puerta de enlace de destino nueva](#)
- [Paso 2: Actualizar las rutas estáticas \(condicional\)](#)
- [Paso 3: Migrar a una nueva gateway](#)
- [Paso 4: Actualizar tablas de enrutamiento de VPC](#)

- [Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino \(condicional\)](#)
- [Paso 6: Actualizar el ASN de la puerta de enlace de cliente \(condicional\)](#)

Paso 1: Crear la puerta de enlace de destino nueva

Antes de realizar la migración a la nueva puerta de enlace de destino, debe configurarla. Para obtener más información acerca de cómo añadir una gateway privada virtual, consulte [the section called “Creación de una gateway privada virtual”](#). Para obtener más información acerca de cómo agregar una gateway de tránsito, consulte [Crear una gateway de tránsito](#) en Gateways de tránsito de Amazon VPC.

Si la nueva puerta de enlace de destino es una puerta de enlace de tránsito, conéctela VPCs a la puerta de enlace de tránsito. Para obtener más información sobre las conexiones de la VPC, consulte [Vinculaciones de una gateway de tránsito a una VPC](#) en Gateways de tránsito de Amazon VPC .

Cuando el destino cambia de una gateway privada virtual a una gateway de tránsito, se puede configurar el ASN de la gateway de tránsito para que tenga el mismo valor que el ASN de la gateway privada virtual. Si prefiere tener un ASN diferente, debe establecer el ASN del dispositivo de gateway de cliente en el ASN de la gateway de tránsito. Para obtener más información, consulte [the section called “Paso 6: Actualizar el ASN de la puerta de enlace de cliente \(condicional\)”](#).

Paso 2: Actualizar las rutas estáticas (condicional)

Este paso es necesario cuando se pasa de una gateway privada virtual con rutas estáticas a una gateway de destino.

Debe eliminar las rutas estáticas antes de migrar a la nueva gateway.

Tip

Mantenga una copia de la ruta estática antes de eliminarla. Tendrá que volver a agregar estas rutas a la gateway de tránsito cuando haya terminado de migrar la conexión de VPN.

Para eliminar una ruta de una tabla de ruteo

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

2. En el panel de navegación, elija Route tables y, a continuación, seleccione la tabla de enrutamiento.
3. En la pestaña Rutas, elija Editar rutas.
4. Elija Eliminar para la ruta estática hacia la puerta de enlace privada virtual.
5. 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, selecciona conexiones Site-to-Site VPN.
3. Elija la conexión de VPN y elija Acciones, Modificar conexión de VPN.
4. En Tipo de destino, elija el tipo de puerta de enlace.
 - a. Si la puerta de enlace de destino nueva es una puerta de enlace privada virtual, elija la puerta de enlace de VPN.
 - b. Si la puerta de enlace de destino nueva es una puerta de enlace de tránsito, elija la puerta de enlace de tránsito.
5. Seleccione Save changes (Guardar cambios).

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

- [ModifyVpnConnection](#)(API de consultas 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 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.

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Puerta de enlace de tránsito	Puerta de enlace de tránsito	Actualice la ruta que contiene el ID de la puerta de enlace de tránsito por el ID de la nueva puerta de enlace de tránsito.

Paso 5: Actualizar el enrutamiento de la puerta de enlace de destino (condicional)

Cuando la nueva puerta de enlace sea una puerta de enlace de tránsito, modifique la tabla de rutas de la puerta de enlace de tránsito para permitir el tráfico entre la VPC y la Site-to-Site VPN. Para obtener más información, consulte [Tablas de enrutamiento de Transit Gateway](#) en Transit Gateways de Amazon VPC.

Si eliminó las rutas estáticas de VPN, debe agregarlas en la tabla de enrutamiento de la gateway de tránsito.

A diferencia de una puerta de enlace privada virtual, una puerta de enlace de tránsito establece el mismo valor para el discriminador de salida múltiple (MED) en todos los túneles de una conexión de VPN. Si está migrando de una puerta de enlace privada virtual a una puerta de enlace de tránsito y ha confiado en el valor del MED para la selección de túnel, le recomendamos que implemente cambios de enrutamiento para evitar problemas de conexión. Por ejemplo, puede anunciar rutas más específicas en su puerta de enlace de tránsito. Para obtener más información, consulte [Tablas de enrutamiento y prioridad de AWS Site-to-Site VPN enrutamiento](#).

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](#).

Modificar AWS Site-to-Site VPN opciones de conexión

Puede modificar las opciones de conexión de su conexión 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.
- El ancho de banda del túnel para la conexión VPN. `standard` admite hasta 1,25 Gbps por túnel, mientras que `large` admite hasta 5 Gbps por túnel. El gran ancho de banda solo está disponible para las conexiones VPN conectadas a una puerta de enlace de tránsito o a Cloud WAN. Para obtener más información, consulte [Túneles de gran ancho de banda](#).

Al modificar las opciones de conexión VPN, las direcciones IP de los puntos finales de la VPN AWS laterales 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, selecciona las conexiones Site-to-Site VPN.
3. Seleccione su conexión de VPN y elija Acciones, Modificar las opciones de conexión de VPN.
4. Introduzca nuevos intervalos de CIDR según sea necesario.
5. 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 consultas de Amazon EC2)

Modifique el ancho de banda del

Puede modificar el ancho de banda del túnel de las conexiones VPN existentes, cambiando entre `standard` (hasta 1,25 Gbps por túnel) y `large` (hasta 5 Gbps por túnel) sin volver a crear las conexiones VPN. Esto le permite realizar una modificación in situ para aumentar o reducir el ancho de banda del túnel en función de sus necesidades.

La capacidad de modificar el ancho de banda del túnel está disponible en las siguientes opciones:

Regiones de AWS

- África (Ciudad del Cabo)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Malasia)
- Asia-Pacífico (Mumbai)
- Asia-Pacífico (Nueva Zelanda)
- Asia-Pacífico (Osaka)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Sídney)
- Asia-Pacífico (Taipéi)
- Asia-Pacífico (Tailandia)
- Asia-Pacífico (Tokio)
- Europa (Fráncfort)
- Europa (Londres)
- Europa (París)
- Europa (España)
- Europa (Estocolmo)
- México (centro)
- América del Sur (São Paulo)
- Este de EE. UU. (Norte de Virginia)
- Este de EE. UU. (Ohio)
- Oeste de EE. UU. (Norte de California)
- AWS GovCloud (US-West)

En las regiones en las que no se admite la modificación del ancho de banda del túnel, primero tendrá que eliminar la conexión VPN y, a continuación, crear una nueva conexión VPN y establecer el ancho de banda del túnel en Grande.

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 VPN Opciones 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 "Service-linked funciones"](#).

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](#).

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

Con una VPN con IP privada, puede implementar IPsec una VPN a través de ella Direct Connect, cifrando el tráfico entre su red local y AWS sin el uso de direcciones IP públicas ni equipos VPN adicionales de terceros.

Uno de los principales usos de la VPN con IP privada Direct Connect es ayudar a los clientes de los sectores financiero, sanitario y federal a cumplir sus objetivos normativos y de cumplimiento. La conexión VPN con IP privada Direct Connect garantiza que el tráfico entre las redes locales AWS y entre ellas sea seguro y privado, lo que permite a los clientes cumplir con sus requisitos normativos y de seguridad.

Beneficios de la VPN de IP privada

- Administración y operaciones de red simplificadas: sin una VPN IP privada, los clientes tienen que implementar VPN y enrutadores de terceros para implementar redes privadas a VPNs través de Direct Connect redes. Con la capacidad de VPN de IP privada, los clientes no tienen que implementar ni administrar su propia infraestructura de VPN. De este modo, se simplifican las operaciones de la red y se reducen los costos.
- Mejora de la seguridad: anteriormente, los clientes tenían que utilizar una interfaz Direct Connect virtual pública (VIF) para cifrar el tráfico Direct Connect, lo que requería direcciones IP públicas para los puntos finales de la VPN. El uso del IPs sistema público aumenta la probabilidad de sufrir ataques externos (DOS), lo que a su vez obliga a los clientes a implementar equipos de seguridad adicionales para proteger la red. Además, un VIF público abre el acceso entre todos los servicios AWS públicos y las redes locales de los clientes, lo que aumenta la gravedad del riesgo. La función de VPN con IP privada permite el cifrado en Direct Connect tránsito VIFs (en lugar de hacerlo público VIFs), además de la posibilidad de configurarlo de forma privada. IPs Esto proporciona conectividad end-to-end privada además del cifrado, lo que mejora la seguridad general.

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

Cómo funciona la VPN de IP privada

La Site-to-Site VPN IP privada funciona a través de una interfaz virtual de Direct Connect tránsito (VIF). Utiliza una Direct Connect puerta de enlace y una puerta de enlace de tránsito para interconectar sus redes locales. Una conexión VPN IP privada tiene puntos de terminación en la pasarela de tránsito, por un AWS lado, y en el dispositivo de puerta de enlace del cliente, en el lado local. Debe asignar direcciones IP privadas a los extremos de los IPsec túneles de la pasarela de tránsito y del dispositivo de puerta de enlace del cliente. Puede usar direcciones IP privadas de uno RFC1918 o varios rangos de IPv4 direcciones RFC6598 privadas.

Adjunta una conexión de VPN de IP privada a una puerta de enlace de tránsito. A continuación, enruta el tráfico entre el adjunto de la VPN y cualquier otra red VPCs (o cualquier otra red) que también esté conectada a la puerta de enlace de tránsito. Esto se hace asociando una tabla de enrutamiento con la conexión de VPN. En la dirección contraria, puede enrutar el tráfico desde su adjunto VPCs a la VPN con IP privada mediante tablas de enrutamiento asociadas a VPCs.

La tabla de rutas asociada al adjunto de la VPN puede ser la misma o diferente de la asociada al Direct Connect adjunto subyacente. Esto le permite enrutar el tráfico cifrado y no cifrado de forma simultánea entre su red VPCs y la local.

Para obtener más información sobre la ruta de tráfico que sale de la VPN, consulte las [políticas de enrutamiento de la interfaz virtual privada y de la interfaz virtual de tránsito](#) en la Guía del usuario de Direct Connect.

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	Steps	Información
Prepare la puerta de enlace de tránsito para Site-to-Site la VPN.	Cree la puerta de enlace de tránsito mediante la consola Amazon Virtual Private	Una puerta de enlace de tránsito es un centro de tránsito de red que puede

Elemento	Steps	Información
	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.	usar para interconectar sus VPCs redes con las locales. Puede crear una nueva puerta de enlace de tránsito o utilizar una ya existente para la conexión de VPN de IP privada. Al crear la puerta de enlace de tránsito, o al modificar una ya existente, se especifica un bloque de CIDR de IP privada para la conexión.  Note Al especificar el bloque de CIDR de la puerta de enlace de tránsito que se va a asociar a su VPN de IP privada, asegúrese de que el bloque de CIDR no se solapa con ninguna dirección 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

Elemento	Steps	Información
		puerta de enlace de cliente.
Cree la Direct Connect puerta de enlace para Site-to-Site la VPN.	Cree la puerta de enlace de Direct Connect mediante la consola de Direct Connect o mediante la línea de comandos o la API. Consulte Crear una puerta de enlace AWS Direct Connect en la Guía Direct Connect del usuario.	Una puerta de enlace Direct Connect le permite conectar interfaces virtuales (VIFs) en varias AWS regiones. Esta puerta de enlace se utiliza para conectarse a VIF.
Cree la asociación de pasarelas de tránsito para la Site-to-Site VPN.	Cree la asociación entre la puerta de enlace de Direct Connect y la puerta de enlace de tránsito mediante la consola de Direct Connect o mediante la línea de comandos o la API. Consulte Asociar o Direct Connect desasociar una pasarela de tránsito en la Guía del Direct Connect usuario.	Después de crear la Direct Connect puerta de enlace, cree una asociación de puerta de enlace de tránsito para la Direct Connect puerta de enlace. Especifique el CIDR de IP privada para la puerta de enlace de tránsito que se identificó anteriormente en la lista de prefijos permitidos.

Tareas

- [Crear una IP privada a AWS Site-to-Site VPN través de Direct Connect](#)

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

Para crear una VPN con IP privada, Direct Connect sigue estos pasos. Antes de crear la VPN de IP privada a través de Direct Connect, debe asegurarse de crear primero una puerta de enlace de

tránsito y una puerta de enlace de Direct Connect. Después de crear las dos puertas de enlace, debe crear una asociación entre las dos. Estos requisitos previos se describen en la tabla siguiente. Una vez que haya creado y asociado las dos puertas de enlace, creará una puerta de enlace para clientes de VPN y una conexión mediante esa asociación.

Requisitos previos

En la siguiente tabla se describen los requisitos previos a la creación de una VPN de IP privada a través de Direct Connect.

Elemento	Steps	Información
Prepare la puerta de enlace de tránsito para la Site-to-Site VPN.	Cree la puerta de enlace de tránsito mediante la consola Amazon Virtual Private Cloud (VPC) o mediante la línea de comandos o la API. Consulte Puertas de enlace de tránsito en la Guía de puertas de enlace de tránsito de Amazon VPC.	Una puerta de enlace de tránsito es un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Puede crear una nueva puerta de enlace de tránsito o utilizar una ya existente para la conexión de VPN de IP privada. Al crear la puerta de enlace de tránsito, o al modificar una ya existente, se especifica un bloque de CIDR de IP privada para la conexión.  Note Al especificar el bloque de CIDR de la puerta de enlace de tránsito que se va a asociar a su VPN de IP privada, asegúrese de que el bloque de CIDR no se solapa

Elemento	Steps	Información
		con ninguna dirección 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 Direct Connect puerta de enlace para Site-to-Site la VPN.	Cree la puerta de enlace de Direct Connect mediante la consola de Direct Connect o mediante la línea de comandos o la API. Consulte Crear una puerta de enlace AWS Direct Connect en la Guía Direct Connect del usuario.	Una puerta de enlace Direct Connect le permite conectar interfaces virtuales (VIFs) en varias AWS regiones. Esta puerta de enlace se utiliza para conectarse a VIF.

Elemento	Steps	Información
Cree la asociación de pasarelas de tránsito para la Site-to-Site VPN.	Cree la asociación entre la puerta de enlace de Direct Connect y la puerta de enlace de tránsito mediante la consola de Direct Connect o mediante la línea de comandos o la API. Consulte Asociar o Direct Connect desasociar una pasarela de tránsito en la Guía del Direct Connect usuario.	Después de crear la Direct Connect puerta de enlace, cree una asociación de puerta de enlace de tránsito para la Direct Connect puerta de enlace. Especifique el CIDR de IP privada para la puerta de enlace de tránsito que se identificó anteriormente en la lista de prefijos permitidos.

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

Una pasarela de clientes es un recurso que se crea en él AWS. Representa el dispositivo de puerta de enlace de cliente en las instalaciones. Cuando crea una pasarela de clientes, proporciona información sobre su dispositivo a AWS. Para obtener más información, consulte [Puerta de enlace de cliente](#).

Para crear una gateway de cliente con la consola

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Puertas de enlace de cliente.
3. Elija Crear puerta de enlace de cliente.
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la puerta de enlace de cliente. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.
5. En BGP ASN, ingrese un número de sistema autónomo (ASN) para protocolo de puerta de enlace fronteriza (BGP) de la puerta de enlace de cliente.
6. En IP address (Dirección IP), ingrese la dirección IP privada de su dispositivo de puerta de enlace de cliente.

⚠ Important

Al configurar la IP AWS privada AWS Site-to-Site VPN, debe especificar sus propias direcciones IP de punto final del túnel mediante las direcciones RFC 1918. No utilice las direcciones point-to-point IP para la interconexión eBGP entre el router de puerta de enlace del cliente y el punto final. Direct Connect AWS recomienda utilizar una interfaz LAN o de bucle invertido en el router de puerta de enlace del cliente como dirección de origen o destino en lugar de conexiones. point-to-point

Para obtener más información sobre la RFC 1918, consulte [Address Allocation for Private Internets](#).

7. (Opcional) En Device (Dispositivo), ingrese un nombre para el dispositivo que aloja esta puerta de enlace de cliente.
8. Elija Crear puerta de enlace de cliente.
9. En el panel de navegación, seleccione las conexiones Site-to-Site VPN.
10. Elija Create VPN Connection (Crear conexión VPN).
11. (Opcional) En la etiqueta de nombre, introduzca un nombre para la conexión Site-to-Site VPN. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.
12. En Target gateway type (Tipo de puerta de enlace de destino), elija Transit gateway (Puerta de enlace de tránsito). A continuación, elija la puerta de enlace de tránsito que identificó anteriormente.
13. En Customer gateway (Puerta de enlace de cliente), seleccione Existing (Existente). A continuación, elija la puerta de enlace de cliente que creó anteriormente.
14. Seleccione una de las opciones de direccionamiento en función de si el dispositivo de gateway de cliente da soporte al protocolo de gateway fronteriza (BGP):
 - Si el dispositivo de gateway de cliente da soporte a BGP, elija Dynamic (requires BGP) (Dinámico [requiere BGP]).
 - Si el dispositivo de gateway de cliente no da soporte a BGP, elija Static (Estático).
15. En la versión Túnel dentro de IP, especifique si los túneles VPN admiten IPv4 IPv6 tráfico.
16. (Opcional) Si especificó IPv4 la versión Túnel dentro de IP, también puede especificar los rangos de IPv4 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado es 0.0.0.0/0.

Si especificó IPv6 la versión Tunnel inside IP, si lo desea, puede especificar los rangos de IPv6 CIDR para la puerta de enlace del cliente y AWS los lados que pueden comunicarse a través de los túneles VPN. El valor predeterminado para ambos rangos es `::/0`.

17. Para el tipo de dirección IP externa, elija PrivateIPv4.
18. En el campo ID del adjunto de transporte, elija el adjunto de la pasarela de tránsito correspondiente a la Direct Connect pasarela correspondiente.
19. Elija Create VPN Connection (Crear conexión VPN).

 Note

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

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

- [CreateCustomerGateway](#) (API de consultas de Amazon EC2)
- [create-customer-gateway](#) (AWS CLI)

Seguridad en AWS Site-to-Site VPN

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de los centros de datos y las arquitecturas de red diseñados para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre AWS usted y usted. El <https://aws.amazon.com/compliance/shared-responsibility-model/> describe estos conceptos como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Third-party los auditores prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los [AWS programas](#) de de . Para obtener más información sobre los programas de cumplimiento que se aplican a las AWS Site-to-Site VPN, consulte [AWS Servicios incluidos en el ámbito de aplicación del programa AWS Servicios incluidos](#) .
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a entender cómo aplicar el modelo de responsabilidad compartida al utilizar Site-to-Site una VPN. Los siguientes temas le muestran cómo configurar la Site-to-Site VPN para cumplir sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger sus recursos de Site-to-Site VPN.

Contenido

- [Mejorado AWS Site-to-Site VPN funciones de seguridad mediante Secrets Manager](#)
- [Protección de datos en AWS Site-to-Site VPN](#)
- [Administración de identidad y acceso para AWS Site-to-Site VPN](#)
- [Resiliencia en AWS Site-to-Site VPN](#)
- [Seguridad de infraestructura en AWS Site-to-Site VPN](#)

Mejorado AWS Site-to-Site VPN funciones de seguridad mediante Secrets Manager

La función Security Rebase de AWS Site-to-Site VPN proporciona capacidades de seguridad mejoradas que le proporcionan un mayor control y visibilidad de sus conexiones de VPN. Una mejora clave es la capacidad de almacenar las claves previamente compartidas (PSK) en el servicio de Site-to-Site VPN, en AWS Secrets Manager lugar de directamente, lo que permite una mejor gestión de los secretos y el cumplimiento de las mejores prácticas de seguridad. La función también incluye una `GetActiveVpnTunnelStatus` API que proporciona visibilidad en tiempo real de los parámetros de seguridad que se utilizan en los túneles VPN activos, incluidos los algoritmos de cifrado, los algoritmos de integridad y los Diffie-Hellman grupos para ambas fases del 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

- [Cambie la clave previamente compartida de Secrets Manager en AWS Site-to-Site VPN](#)
- [Cambie el modo de almacenamiento de claves previamente compartidas en AWS Site-to-Site VPN](#)

Cambie la clave previamente compartida 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, selecciona las conexiones Site-to-Site VPN.
3. Seleccione la conexión Site-to-Site VPN y elija Acciones, Modificar las opciones del túnel VPN.
4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. En 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.

Cambie el modo de almacenamiento de claves previamente compartidas 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, selecciona las conexiones Site-to-Site VPN.
3. Seleccione la conexión Site-to-Site VPN y elija Acciones, Modificar las opciones del túnel VPN.

4. En Dirección IP externa del túnel de VPN, elija la IP del punto de conexión del túnel de VPN.
5. En Almacenamiento de Pre-shared claves, elija uno de los siguientes tipos de almacenamiento de claves previamente compartidas.
 - Estándar: la clave previamente compartida se almacena directamente en el Site-to-Site servicio de VPN.
 - Secrets Manager: la clave 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 previamente compartida 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 previamente compartida se elimina del servicio VPN Site-to-Site
- 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](#) se aplica a la protección de datos en las AWS Site-to-Site VPN. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Eres responsable de mantener el control sobre el contenido alojado en esta infraestructura. También eres responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las [Preguntas frecuentes sobre privacidad de datos](#) y los . Para obtener más información sobre la protección de datos en Europa, consulte el [Centro del Reglamento General de Protección de Datos \(RGPD\)](#).

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS las credenciales y configure usuarios individuales con AWS IAM Identity Center o AWS Identity and Access

Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utiliza la autenticación multifactor (MFA) en cada cuenta.
- Se utiliza SSL/TLS para comunicarse con AWS los recursos. Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte [Cómo trabajar con CloudTrail senderos](#) en la Guía del AWS CloudTrail usuario.
- Utilice soluciones de AWS cifrado, junto con todos los controles de seguridad predeterminados Servicios de AWS.
- Utiliza servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger la información confidencial almacenada en Amazon S3.
- Si necesita módulos criptográficos validados por FIPS 140-3 para acceder a AWS través de una interfaz de línea de comandos o una API, utilice un punto final FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte [Estándar de procesamiento de la información federal \(FIPS\) 140-3](#).

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye cuando trabaja con Site-to-Site una VPN u otra Servicios de AWS mediante la consola, la API o los SDK. AWS CLI AWS Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para los nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Privacidad del tráfico entre redes

Una conexión Site-to-Site VPN conecta de forma privada la VPC a la red local. Los datos que se transfieren entre su VPC y su red se direccionan a través de una conexión de VPN cifrada para ayudarlo a mantener la confidencialidad y la integridad de los datos en tránsito. Amazon 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 Site-to-Site VPN consta de dos túneles VPN IPsec cifrados que enlazan AWS con tu red. El tráfico de cada túnel se puede cifrar con AES128 o AES256 y utilizar Diffie-Hellman grupos para el intercambio de claves, lo que proporciona un secreto directo perfecto. AWS se autentica con las funciones de hash SHA1 o SHA2.

Las instancias de la VPC no requieren una dirección IP pública para conectarse a los recursos del otro lado de la conexión de la Site-to-Site VPN. Las instancias pueden enrutar su tráfico de Internet a través de la conexión Site-to-Site VPN a la red local. A continuación, pueden obtener acceso a Internet a través de los puntos de tráfico salientes y de sus dispositivos de monitoreo y seguridad de la red.

Consulte los siguientes temas para obtener más información:

- [Opciones de túnel para su AWS Site-to-Site VPN conexión](#): proporciona información sobre las opciones de IPsec e Intercambio de claves de Internet (IKE) disponibles para cada túnel.
- [AWS Site-to-Site VPN Opciones de autenticación de túneles de](#): proporciona información sobre las opciones de autenticación de los puntos de enlace del túnel de VPN.
- [Requisitos para un AWS Site-to-Site VPN Dispositivo de gateway de cliente](#): proporciona información sobre los requisitos del dispositivo de gateway de cliente en su extremo de la conexión de VPN.
- [Comunicación segura entre AWS Site-to-Site VPN conexiones mediante VPN CloudHub](#): Si tienes varias conexiones Site-to-Site VPN, puedes proporcionar una comunicación segura entre tus sitios locales mediante la AWS VPN. CloudHub

Administración de identidad y acceso para AWS Site-to-Site VPN

AWS Identity and Access Management (IAM) es un sistema Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. Los administradores de IAM controlan quién puede autenticarse (iniciar sesión) y quién puede autorizarse (tener permisos) para usar Site-to-Site los recursos de la VPN. El IAM es un Servicio de AWS servicio que puede utilizar sin coste adicional.

Temas

- [Público](#)
- [Autenticación con identidades](#)

- [Administración del acceso con políticas](#)
- [Cómo AWS Site-to-Site La VPN funciona con IAM](#)
- [Identity-based ejemplos de políticas para AWS Site-to-Site VPN](#)
- [Resolución de problemas AWS Site-to-Site Identidad y acceso a la VPN](#)
- [AWS políticas gestionadas para VPN Site-to-Site](#)
- [Uso de funciones vinculadas a servicios para la VPN Site-to-Site](#)

Público

La forma de usar AWS Identity and Access Management (IAM) varía según la función que desempeñes:

- Usuario del servicio: solicite permisos al administrador si no puede acceder a las características (consulte [Resolución de problemas AWS Site-to-Site Identidad y acceso a la VPN](#)).
- Administrador del servicio: determine el acceso de los usuarios y envíe las solicitudes de permiso (consulte [Cómo AWS Site-to-Site La VPN funciona con IAM](#)).
- Administrador de IAM: escribe las políticas para administrar el acceso (consulte [Identity-based ejemplos de políticas para AWS Site-to-Site VPN](#)).

Autenticación con identidades

La autenticación es la forma en que inicias sesión AWS con tus credenciales de identidad. Debe autenticarse como usuario de Usuario raíz de la cuenta de AWS IAM o asumir una función de IAM.

Puede iniciar sesión como una identidad federada con las credenciales de una fuente de identidad, como AWS IAM Identity Center (IAM Identity Center), la autenticación de inicio de sesión único o las credenciales. Google/Facebook Para obtener más información sobre el inicio de sesión, consulte [Cómo iniciar sesión en la 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.

Cuenta de AWS usuario raíz

Al crear una Cuenta de AWS, se comienza con una identidad de inicio de sesión denominada usuario Cuenta de AWS raíz, que tiene acceso completo a todos los Servicios de AWS recursos. Se

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 Servicios de AWS mediante credenciales temporales.

Una identidad federada es un usuario del directorio empresarial, del proveedor de identidades web o al Directory Service que se accede Servicios de AWS mediante credenciales de una fuente de identidad. Las identidades federadas asumen roles que proporcionan credenciales temporales.

Para una administración de acceso centralizada, se recomienda 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 el uso de credenciales temporales en lugar de usuarios de IAM con credenciales de larga duración. Para obtener más información, consulte [Exigir a los usuarios humanos que utilicen la federación con un proveedor de identidad para acceder AWS mediante credenciales temporales](#) en la Guía del usuario de IAM.

Un [grupo de IAM](#) especifica un conjunto de usuarios de IAM y facilita la administración de los permisos para grupos grandes 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 un rol de usuario a uno de IAM \(consola\)](#) o llamando a una AWS CLI operación de AWS API. 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 usuario federado, 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 del acceso con políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política define los permisos cuando están asociados a una identidad o un recurso. AWS evalúa estas políticas cuando un director hace una solicitud. La mayoría de las políticas se almacenan AWS como documentos JSON. Para obtener más información sobre los documentos de políticas de JSON, consulte [Información general de políticas de 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 agrega a roles, que los usuarios pueden asumir posteriormente. Las políticas de IAM definen permisos independientemente del método que se utilice para realizar la operación.

Identity-based políticas

Identity-based las políticas son documentos de política de permisos de JSON que se adjuntan a una identidad (usuario, grupo o rol). Estas políticas controlan qué acciones pueden realizar las identidades, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política basada en la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) en la Guía del usuario de IAM.

Identity-based las políticas pueden ser políticas integradas (integradas directamente en una sola identidad) o políticas administradas (políticas independientes asociadas a varias identidades). Para obtener información sobre cómo elegir entre políticas administradas e insertadas, consulte [Selección entre políticas administradas y políticas insertadas](#) en la Guía del usuario de IAM.

Resource-based políticas

Resource-based las políticas son documentos de políticas de JSON que se adjuntan a un recurso. Los ejemplos incluyen 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 basada en recursos.

Resource-based las políticas son políticas en línea que se encuentran en ese servicio. No puedes usar políticas AWS gestionadas de IAM en una política basada en recursos.

Otros tipos de políticas

AWS admite tipos de políticas adicionales que pueden establecer los permisos máximos que conceden los tipos de políticas más comunes:

- Límites de permisos: establecen los permisos máximos que una política basada en 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): definen 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 obtener más información, consulte [Políticas de sesión](#) en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la [lógica de evaluación de políticas](#) en la Guía del usuario de IAM.

Cómo AWS Site-to-Site La VPN funciona con IAM

Antes de utilizar IAM para gestionar el acceso a la Site-to-Site VPN, infórmese sobre las funciones de IAM disponibles para su uso con la VPN. Site-to-Site

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

Característica de IAM	Site-to-Site Soporte de VPN
Identity-based políticas	Sí
Resource-based políticas	No

Característica de IAM	Site-to-Site Soporte de VPN
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
Service-linked roles	Sí

Para obtener una visión general del funcionamiento de la Site-to-Site VPN y otros AWS servicios con la mayoría de las funciones de IAM, consulte [AWS los servicios que funcionan con IAM](#) en la Guía del usuario de IAM.

Identity-based políticas de VPN Site-to-Site

Compatibilidad con las políticas basadas en identidad: sí

Identity-based las políticas son documentos de política de permisos de JSON que puedes adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. 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 la identidad, consulte [Definición de permisos de IAM personalizados con políticas administradas por el cliente](#) 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 la política de JSON de IAM](#) en la Guía del usuario de IAM.

Identity-based ejemplos de políticas para VPN Site-to-Site

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte [Identity-based ejemplos de políticas para AWS Site-to-Site VPN](#)

Resource-based políticas dentro de la VPN Site-to-Site

Admite políticas basadas en recursos: no

Resource-based las políticas son documentos de políticas de JSON que se adjuntan 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 basada en recursos. Los principales pueden incluir cuentas, usuarios, roles, usuarios federados o. Servicios de AWS

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

Acciones políticas para la VPN Site-to-Site

Compatibilidad con las acciones de políticas: sí

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

El elemento `Action` de una política JSON describe las acciones que puede utilizar para conceder o denegar el acceso en una política. Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de la Site-to-Site VPN, consulte [las acciones definidas por la AWS Site-to-Site VPN](#) en la Referencia de autorización del servicio.

Las acciones políticas de la Site-to-Site VPN utilizan el siguiente prefijo antes de la acción:

```
ec2
```

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [  
    "ec2:action1",  
    "ec2:action2"  
]
```

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte [Identity-based ejemplos de políticas para AWS Site-to-Site VPN](#)

Recursos de políticas para VPN Site-to-Site

Compatibilidad con los recursos de políticas: sí

Los administradores pueden usar las políticas de AWS JSON para especificar quién tiene acceso a qué. Es decir, qué entidad principal 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 \(ARN\)](#). En el caso de 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 [los recursos definidos por la AWS Site-to-Site VPN](#) en la Referencia de autorización de servicios. Para saber con qué acciones puede especificar el ARN de cada recurso, consulte [Acciones definidas por AWS Site-to-Site](#) la VPN.

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte [Identity-based ejemplos de políticas para AWS Site-to-Site VPN](#)

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

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

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

El elemento `Condition` especifica cuándo se ejecutan las instrucciones en función de criterios definidos. Puede 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 AWS globales, consulte las claves de [contexto de condición AWS globales](#) en la Guía del usuario de IAM.

Para ver una lista de las claves de condición de la Site-to-Site VPN, consulte las [claves de condición de la AWS Site-to-Site VPN](#) en la Referencia de autorización de servicios. Para saber con qué acciones y recursos puede utilizar una clave condicionada, consulte [Acciones definidas por la AWS Site-to-Site VPN](#).

Para ver ejemplos de políticas de Site-to-Site VPN basadas en la identidad, consulte [Identity-based ejemplos de políticas para AWS Site-to-Site VPN](#)

ACL en una VPN Site-to-Site

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 VPN Site-to-Site

Compatibilidad con ABAC (etiquetas en las políticas): no

Attribute-based el control de acceso (ABAC) es una estrategia de autorización que define los permisos en función de unos atributos denominados etiquetas. Puede adjuntar etiquetas a las entidades y AWS los recursos de IAM y, a continuación, diseñar políticas de ABAC para permitir las operaciones cuando la etiqueta del director 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 una VPN Site-to-Site

Compatibilidad con credenciales temporales: sí

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

Cross-service permisos principales para la Site-to-Site VPN

Admite sesiones de acceso directo (FAS): sí

Las sesiones de acceso directo (FAS) utilizan los permisos del operador principal que realiza la llamada Servicio de AWS, junto con los de solicitud, Servicio de AWS para realizar solicitudes a los servicios descendentes. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte [Sesiones de acceso directo](#).

Funciones de servicio para la VPN Site-to-Site

Compatible 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 [Crear un rol para delegar permisos a un Servicio de AWS](#) en la Guía del usuario de IAM.

Warning

Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de la Site-to-Site VPN. Edite las funciones de servicio solo cuando la Site-to-Site VPN proporcione instrucciones para hacerlo.

Service-linked funciones para la Site-to-Site VPN

Compatible con roles vinculados al servicio: sí

Un rol vinculado a un servicio es un tipo de rol de servicio que está vinculado a un. Servicio de AWS El servicio puede asumir la función de realizar una acción en su nombre. Service-linked las funciones aparecen en su nombre Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

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 una Yes en la columna de Service-linked funciones. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Identity-based ejemplos de políticas para AWS Site-to-Site VPN

De forma predeterminada, los usuarios y los roles no tienen permiso para crear o modificar los recursos de la 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 identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte [Creación de políticas de IAM \(consola\)](#) en la Guía del usuario de IAM.

Para obtener más información sobre las acciones y los tipos de recursos definidos por la Site-to-Site VPN, incluido el formato de los ARN de cada uno de los tipos de recursos, consulte [Acciones, recursos y claves de condición de la AWS Site-to-Site VPN](#) en la Referencia de autorización de servicios.

Temas

- [Prácticas recomendadas sobre las políticas](#)
- [Uso de la consola VPN Site-to-Site](#)
- [Describa las conexiones Site-to-Site VPN específicas](#)
- [Cree y describa los recursos necesarios para una AWS Site-to-Site VPN conexión](#)

Prácticas recomendadas sobre las políticas

Identity-based las políticas determinan si alguien puede crear, acceder o eliminar los recursos de Site-to-Site VPN de su 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:

- Comience con las políticas AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Con el fin de obtener más información, 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, puede escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo 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.
- Requerir autenticación multifactor (MFA): si tiene un escenario que requiere usuarios de IAM o un usuario raíz en Cuenta de AWS su cuenta, active la MFA para mayor seguridad. Para exigir la MFA cuando se invoquen las operaciones de la API, añada condiciones de MFA a sus políticas. Para más información, consulte [Acceso seguro a la API con MFA](#) en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte [Prácticas recomendadas de seguridad en IAM](#) en la Guía del usuario de IAM.

Uso de la consola VPN Site-to-Site

Para acceder a la consola AWS Site-to-Site VPN, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle enumerar y ver detalles sobre los recursos de Site-to-Site VPN de su propiedad Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que concedas permisos mínimos de consola a los usuarios que solo realicen llamadas a la API AWS CLI o a la AWS API. En su lugar, permita el acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para garantizar que los usuarios y los roles puedan seguir utilizando la consola Site-to-Site VPN, vincule también la Site-to-Site VPN AmazonVPCFullAccess o la política AmazonVPCReadOnlyAccess AWS gestionada a las entidades. Para obtener más información, consulte [Adición de permisos a un usuario](#) en la Guía del usuario de IAM:

Describe las conexiones Site-to-Site VPN específicas

JSON

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

Cree y describa los recursos necesarios para una AWS Site-to-Site VPN conexión

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"
        }
      }
    }
  ]
}
```

Resolución de problemas AWS Site-to-Site Identidad y acceso a la VPN

Utilice la siguiente información como ayuda para diagnosticar y solucionar los problemas más comunes que pueden surgir al trabajar con Site-to-Site VPN e IAM.

Temas

- [No estoy autorizado a realizar ninguna acción en la VPN Site-to-Site](#)
- [No estoy autorizado a realizar tareas como: PassRole](#)
- [Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mis recursos de Site-to-Site VPN](#)

No estoy autorizado a realizar ninguna acción en la VPN Site-to-Site

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *my-example-widget*, pero no tiene los permisos ficticios `ec2:GetWidget`.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
ec2:GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *my-example-widget* mediante la acción `ec2:GetWidget`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

No estoy autorizado a realizar tareas como: PassRole

Si recibes un mensaje de error que indica que no estás autorizado a realizar la `iam:PassRole` acción, debes actualizar tus políticas para que puedas transferir una función a la Site-to-Site VPN.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada al servicio. Para ello, debe tener permisos para transferir la función al servicio.

El siguiente ejemplo de error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en la 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 la función al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su AWS administrador. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi Cuenta de AWS para acceder a mis recursos de Site-to-Site VPN

Se puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Se 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 saber si la Site-to-Site VPN admite estas funciones, consulte [Cómo AWS Site-to-Site La VPN funciona con IAM](#).
- Para obtener información sobre cómo proporcionar acceso a los recursos de su Cuentas de AWS propiedad, consulte [Proporcionar acceso a un usuario de IAM en otro usuario de su propiedad Cuenta de AWS en](#) la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta [Cómo proporcionar acceso a recursos que Cuentas de AWS son propiedad de terceros](#) en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulte [Proporcionar acceso a usuarios autenticados externamente \(identidad federada\)](#) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre las políticas basadas en roles y en recursos para el acceso entre cuentas, consulte [Acceso a recursos entre cuentas en IAM](#) en la Guía del usuario de IAM.

AWS políticas gestionadas para VPN Site-to-Site

Para añadir permisos a usuarios, grupos y roles, es más fácil usar políticas AWS administradas que escribirlas tú mismo. Se necesita tiempo y experiencia para [crear políticas administradas por el cliente de IAM](#) que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puedes usar nuestras políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en tu AWS cuenta. Para obtener más información sobre las políticas AWS administradas, consulte las [políticas AWS administradas](#) en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas gestionadas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política administrada de AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política `ReadOnlyAccess` AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

AWS política gestionada: `AWSVPCS2SVpnServiceRolePolicy`

Puede asociar la política `AWSVPCS2SVpnServiceRolePolicy` a las identidades de IAM. Esta política permite a la Site-to-Site VPN administrar un AWS Secrets Manager secreto dentro de la Site-to-Site VPN. Para obtener más información, consulte [the section called “Cómo utilizar roles vinculados a servicios”](#).

Para ver los permisos de esta política, consulte [AWSVPCS2SVpnServiceRolePolicy](#) en la Referencia de la política administrada de AWS .

Site-to-Site La VPN se actualiza a AWS políticas administradas

Consulta los detalles sobre las actualizaciones de las políticas AWS gestionadas de las Site-to-Site VPN desde que este servicio comenzó a registrar estos cambios en mayo de 2025.

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

Uso de funciones vinculadas a servicios para la VPN Site-to-Site

AWS Site-to-Site La VPN usa roles AWS Identity and Access Management vinculados al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a la VPN. Site-to-Site Service-linked Las funciones están predefinidas por la Site-to-Site VPN e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en tu nombre.

Un rol vinculado a un servicio facilita la configuración de la Site-to-Site VPN, ya que no es necesario añadir manualmente los permisos necesarios. Site-to-Site La VPN define los permisos de sus funciones vinculadas al servicio y, a menos que se defina lo contrario, solo la Site-to-Site VPN puede asumir sus funciones. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de Site-to-Site VPN porque no puede eliminar inadvertidamente el permiso de acceso a los recursos.

Service-linked permisos de rol para la VPN Site-to-Site

Site-to-Site La VPN usa el rol vinculado al servicio denominado `AWSServiceRoleForVPCS2SVPN`: Permita que la Site-to-Site VPN cree y administre los recursos relacionados con sus conexiones de VPN.

El rol `AWSServiceRoleForVPCS2SVPN` vinculado al servicio confía en que el siguiente servicio asuma el rol:

- `s2svpn.amazonaws.com`

Este rol vinculado al servicio usa la política administrada `AWSVPCS2SVpnServiceRolePolicy` para completar las siguientes acciones en los recursos especificados:

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

Para ver los permisos de esta política, consulte [AWSVPCS2SVpnServiceRolePolicy](#) en la Referencia de la política administrada de AWS .

Cree un rol vinculado a un servicio para la VPN Site-to-Site

No necesita crear manualmente un rol vinculado a servicios. Al crear una pasarela de cliente con un certificado privado de ACM asociado en la Consola de administración de AWS, la o la AWS API AWS CLI, la Site-to-Site VPN crea automáticamente la función vinculada al servicio.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al crear una pasarela de clientes con un certificado privado de ACM asociado, la Site-to-Site VPN vuelve a crear la función vinculada al servicio para usted.

Edita un rol vinculado a un servicio para la VPN Site-to-Site

Site-to-Site La VPN no le permite editar el rol vinculado al `AWSServiceRoleForVPCS2SVPN` servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte la [Descripción sobre cómo editar un rol vinculado al servicio](#) en la Guía del usuario de IAM.

Elimine un rol vinculado a un servicio para la VPN Site-to-Site

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se supervise ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

 Note

Si el servicio de Site-to-Site VPN utiliza el rol al intentar eliminar los recursos, es posible que la eliminación no se realice correctamente. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos de Site-to-Site VPN utilizados por el `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. Esto garantiza que no pueda eliminar inadvertidamente el permiso de acceso a los certificados ACM que utilizan las conexiones VPN. Site-to-Site

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al servicio. `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 AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS](#)

Además de la infraestructura AWS global, la Site-to-Site VPN ofrece funciones que ayudan a satisfacer sus necesidades de respaldo y resiliencia de datos.

Dos túneles por conexión de VPN

Una conexión Site-to-Site VPN consta de dos túneles, cada uno de los cuales termina en una zona de disponibilidad diferente, para proporcionar una mayor disponibilidad a la VPC. Si se produce un

fallo en un dispositivo interno AWS, la conexión VPN pasa automáticamente al segundo túnel para que el acceso no se interrumpa. De vez en cuando, AWS también realiza un mantenimiento rutinario de la conexión VPN, lo que puede desactivar brevemente uno de los dos túneles de la conexión VPN. Para obtener más información, consulte [AWS Site-to-Site VPN reemplazos de puntos finales de túneles](#). Al configurar su gateway de cliente, por tanto es importante que configure ambos túneles.

Redundancia

Para protegerte de una pérdida de conectividad en caso de que tu pasarela de cliente deje de estar disponible, puedes configurar una segunda conexión Site-to-Site VPN. Para obtener más información, consulte la siguiente documentación sobre :

- [Redundante AWS Site-to-Site VPN conexiones para conmutación por error](#)
- [Opciones de conectividad de Amazon Virtual Private Cloud](#)
- [Creación de una infraestructura de Multi-VPC AWS red escalable y segura](#)

Seguridad de infraestructura en AWS Site-to-Site VPN

Como servicio gestionado, la AWS Site-to-Site VPN está protegida por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las llamadas a la API AWS publicadas para acceder a la Site-to-Site VPN a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Paquetes de cifrado con perfecto secreto directo (PFS), como el DHE (Ephemeral) o el ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Diffie-Hellman La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Supervisar una AWS Site-to-Site VPN conexión

La supervisión es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el rendimiento de la AWS Site-to-Site VPN conexión. Debe recopilar datos de supervisión de todas las partes de la solución de para que, dado el caso, le resulte más sencillo depurar un error multipunto. Sin embargo, antes de comenzar a monitorear su conexión Site-to-Site VPN, debe crear un plan de monitoreo que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la supervisión?
- ¿Qué recursos va a supervisar?
- ¿Con qué frecuencia va a supervisar estos recursos?
- ¿Qué herramientas de supervisión va a utilizar?
- ¿Quién se encargará de realizar las tareas de supervisión?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del desempeño de VPN normal en su entorno. Para ello se mide el desempeño en distintos momentos y bajo distintas condiciones de carga. A medida que monitoree 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 Site-to-Site VPN registros](#)
- [Supervise AWS Site-to-Site VPN los túneles con Amazon CloudWatch](#)
- [AWS Health y AWS Site-to-Site VPN eventos](#)

Herramientas de supervisión

AWS proporciona varias herramientas que puede utilizar para supervisar una conexión Site-to-Site VPN. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de supervisión automatizadas

Puede utilizar las siguientes herramientas de supervisión automática para vigilar una conexión Site-to-Site VPN e informar cuando algo vaya mal:

- Amazon CloudWatch Alarms: observe una sola métrica durante un período de tiempo que especifique y realice una o más acciones en función del valor de la métrica en relación con un umbral determinado durante varios períodos de tiempo. La acción es una notificación que se envía a un tema de Amazon SNS. CloudWatch las alarmas no invocan acciones simplemente porque se encuentran en un estado determinado; el estado debe haber cambiado y se ha mantenido durante un número específico de períodos. Para obtener más información, consulte [Supervise AWS Site-to-Site VPN los túneles con Amazon CloudWatch](#).
- AWS CloudTrail Supervisión de registros: comparta archivos de registro entre cuentas, supervise los archivos de CloudTrail registro en tiempo real enviándolos a CloudWatch Logs, cree aplicaciones de procesamiento de registros en Java y valide que los archivos de registro no hayan cambiado después de la entrega. CloudTrail Para obtener más información, consulte [Uso de llamadas a la API de Registro AWS CloudTrail](#) en la Referencia de API de Amazon EC2 y [Uso de archivos de CloudTrail registro](#) en la Guía del AWS CloudTrail usuario.
- AWS Health eventos: reciba alertas y notificaciones relacionadas con los cambios en el estado de sus túneles de Site-to-Site VPN, las recomendaciones de configuración recomendadas o cuando se acerque a los límites de escalado. Utilice los eventos de [Personal Health Dashboard](#) para activar conmutaciones por error automatizadas, reducir el tiempo de resolución de problemas y optimizar las conexiones para disfrutar de una alta disponibilidad. Para obtener más información, consulte [AWS Health y AWS Site-to-Site VPN eventos](#).

Herramientas de supervisión manuales

Otra parte importante de la supervisión de una conexión Site-to-Site VPN consiste en supervisar manualmente los elementos que no cubren CloudWatch las alarmas. Los paneles de Amazon VPC y de CloudWatch consola ofrecen una at-a-glance visión del estado de su entorno. AWS

 Note

En la consola de Amazon VPC, es posible que los parámetros de estado del túnel Site-to-Site VPN, como «Estado» y «Último cambio de estado», no reflejen los cambios de estado transitorios ni los cambios momentáneos del túnel. Se recomienda utilizar CloudWatch métricas y registros para actualizar de forma pormenorizada los cambios en el estado del túnel.

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

Además, puede CloudWatch hacer lo siguiente:

- Crear [paneles personalizados](#) para monitorizar los servicios que le interesan
- Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias
- Busque y explore todas sus métricas AWS de recursos
- Crear y editar las alarmas de notificación de problemas

AWS Site-to-Site VPN registros

AWS Site-to-Site VPN los registros le proporcionan una mayor visibilidad de sus despliegues de Site-to-Site VPN. Con esta función, tiene acceso a los registros de conexiones Site-to-Site VPN que proporcionan detalles sobre el establecimiento del túnel de seguridad IP (IPsec), las negociaciones sobre el intercambio de claves de Internet (IKE), los mensajes del protocolo de detección de puntos muertos (DPD), el estado del protocolo Border Gateway (BGP) y las actualizaciones de enrutamiento.

Site-to-Site Los registros de VPN se pueden publicar en Amazon CloudWatch Logs. Esta función proporciona a los clientes una forma única y coherente de acceder a los registros detallados de todas sus conexiones Site-to-Site VPN y analizarlos.

Temas

- [Ventajas de los registros de Site-to-Site VPN](#)
- [Restricciones de tamaño de la política de recursos de Amazon CloudWatch Logs](#)
- [Site-to-Site Contenido del registro de VPN](#)
- [Ejemplo de formato de registro para los registros BGP de Tunnel](#)
- [Requisitos de IAM para publicar en los registros CloudWatch](#)
- [Vea la configuración AWS Site-to-Site VPN de los registros](#)
- [Habilitar los registros AWS Site-to-Site VPN](#)
- [Inhabilitar AWS Site-to-Site VPN los registros](#)

Ventajas de los registros de Site-to-Site VPN

- Solución de problemas simplificada con la Site-to-Site VPN: los registros de la VPN le ayudan a detectar las discrepancias de configuración entre AWS el dispositivo de puerta de enlace del cliente y a solucionar los problemas iniciales de conectividad de la VPN. Las conexiones de VPN pueden cambiar de forma intermitente con el tiempo debido a ajustes mal configurados (como tiempos de espera mal ajustados), puede haber problemas en las redes de transporte subyacentes (como el tiempo de Internet) o los cambios de enrutamiento o los errores de ruta pueden provocar la interrupción de la conectividad a través de VPN. Esta característica le permite diagnosticar con precisión la causa de los errores de conexión intermitentes y ajustar la configuración del túnel de bajo nivel para lograr un funcionamiento fiable.
- AWS Site-to-Site VPN Visibilidad centralizada: los registros de Site-to-Site VPN pueden proporcionar registros de actividad de túneles y de enrutamiento BGP en todos los tipos de conexiones de Site-to-Site VPN. Esta función proporciona a los clientes una forma única y coherente de acceder a los registros detallados de todas sus conexiones Site-to-Site VPN y analizarlos.
- Seguridad y conformidad: los registros de Site-to-Site VPN se pueden enviar a Amazon CloudWatch Logs para un análisis retrospectivo del estado y la actividad de la conexión VPN a lo largo del tiempo. Esto puede ayudarle a cumplir con los requisitos reglamentarios y de conformidad.

Restricciones de tamaño de la política de recursos de Amazon CloudWatch Logs

CloudWatch Las políticas de recursos de Logs están limitadas a 5120 caracteres. Cuando CloudWatch Logs detecta que una política se acerca a este límite de tamaño, habilita automáticamente los grupos de registros que comiencen por `/aws/vendedlogs/`. Cuando habilita el registro, la Site-to-Site VPN debe actualizar su política de recursos de CloudWatch registros con el grupo de registros que especifique. Para evitar alcanzar el límite de tamaño de la política de recursos de CloudWatch registros, añada el prefijo a los nombres de los grupos de registros. `/aws/vendedlogs/`

Site-to-Site Contenido del registro de VPN

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

Campo	Description (Descripción)
VpnLogCreationTimestamp (event_timestamp)	Marca de tiempo de creación del registro en formato de época.
VpnLogCreationTimestampReadable (timestamp)	Marca de tiempo de creación del registro en formato de tiempo legible por humanos.
Túnel DPDEnabled () dpd_enabled	Estado habilitado del protocolo de detección de pares muertos (verdadero/falso).
CGWNATTDetectionEstado del túnel (nat_t_detected)	NAT-T detectado en el dispositivo de puerta de enlace de cliente (verdadero/falso).
IKEPhase1Estado del túnel (ike_phase1_state)	Estado del protocolo de fase 1 de IKE (Establecido Cambio de clave Negociación Inactivo).
IKEPhase2Estado del túnel (ike_phase2_state)	Estado del protocolo de fase 2 de IKE (Establecido Cambio de clave Negociación Inactivo).

Campo	Description (Descripción)
VpnLogDetail (details)	Mensajes detallados para IPsec los protocolos IKE y DPD.

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

Campo	Description (Descripción)
resource_id	Un identificador único para identificar el túnel y la conexión VPN a la que está asociado el registro.
event_timestamp	Marca de tiempo de creación del registro en formato de época.
timestamp	Marca de tiempo de creación del registro en formato de tiempo legible por humanos.
type	Tipo de evento de registro de BGP ()BGPStatus . RouteStatus
status	actualización de estado para un tipo específico o de registro de eventos (BGPStatus: ARRIBA ABAJO) (RouteStatus: ANUNCIADO {la ruta la anunció el par} ACTUALIZADO: {el par actualizó la ruta existente} RETIRADA: {el par retiró la ruta}).
message	Proporciona detalles adicionales sobre el registro de eventos y su estado. Este campo le ayudará a entender por qué BGPStatus no se utiliza la ruta y qué atributos se intercambiaron en el RouteStatus mensaje.

Contenido

- [IKEv1 Mensajes de error](#)
- [IKEv2 Mensajes de error](#)
- [IKEv2 Mensajes de negociación](#)
- [Mensajes de estado del BGP](#)
- [Mensajes de estado de la ruta](#)

IKEv1 Mensajes de error

Mensaje	Explicación
El par no responde: declarar muerto al par	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
AWS El descifrado de la carga útil del túnel no se pudo realizar debido a que la clave previamente compartida no era válida	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.
No se encontró ninguna propuesta que coincidiera AWS	El punto de conexión de AWS VPN no admite los atributos propuestos para la fase 1 (cifrado, hash y grupo DH), por ejemplo, 3DES.
No se encontró ninguna coincidencia de propuesta. Notificación con la opción «No se ha elegido ninguna propuesta»	Se intercambia el mensaje de error No Propuesta elegida entre pares para indicar que se Proposals/Policiés debe configurar la correcta para la fase 2 en IKE Peers.
AWS tunnel recibió el comando DELETE para la SA de fase 2 con el SPI: xxxx	CGW ha enviado el mensaje Delete_SA para la fase 2.
AWS tunnel recibió un DELETE para IKE_SA de CGW	CGW ha enviado el mensaje Delete_SA para la fase 1.

IKEv2 Mensajes de error

Mensaje	Explicación
AWS Se agotó el tiempo de espera del DPD del túnel después de la retransmisión de {retry_count}	El par no ha respondido a los mensajes de DPD, por lo que se ha impuesto la acción de tiempo de espera del DPD.
AWS El túnel recibió el comando DELETE para IKE_SA de CGW	El par ha enviado el mensaje Delete_SA para Parent/IKE_SA.
AWS tunnel recibió DELETE para la SA de fase 2 con el SPI: xxxx	El par ha enviado el mensaje Delete_SA para CHILD_SA.
AWS El túnel detectó una colisión (CHILD_RE KEY) como CHILD_DELETE	CGW ha enviado el mensaje Delete_SA para la SA activa, a la que se le está cambiando la clave.
AWS La SA redundante del túnel (CHILD_SA) se está eliminando debido a una colisión detectada	Debido a una colisión, si SAs se generan redundantes, Peers cerrará la SA redundant e después de hacer coincidir los valores de nonce según la RFC.
AWS No se pudo establecer la fase 2 del túnel mientras se mantenía la fase 1	El par no pudo establecer CHILD_SA debido a un error de negociación, por ejemplo, a una propuesta incorrecta.
AWS: Selector de tráfico: TS_UNACCE PTABLE: recibido del agente de respuesta	Peer ha propuesto un Selectors/Encryption dominio de tráfico incorrecto. Los pares deben configurarse con el mismo y el correcto CIDRs.
AWS el túnel envía AUTHENTICATION_FAILED como respuesta	El par no puede autenticar al par al verificar el contenido del mensaje IKE_AUTH
AWS tunnel detectó una falta de coincidencia de claves previamente compartidas con cgw: xxxx	Se debe configurar la misma clave previamente compartida en ambos pares de IKE.

Mensaje	Explicación
AWS Tiempo de espera del túnel: eliminar el IKE_SA de fase 1 no establecido con cgw: xxxx	La eliminación de IKE_SA semiabierto como par no ha continuado con las negociaciones
No se encontró ninguna coincidencia de propuesta. Notificación con la opción «No se ha elegido ninguna propuesta»	Los pares no intercambian ningún mensaje de error de propuesta elegida para informar que las propuestas correctas se deben configurar en pares de IKE.
No se encontró ninguna propuesta que coincidiera AWS	Los atributos propuestos para la fase 1 o la fase 2 (cifrado, hash y grupo DH) no son compatibles con AWS VPN Endpoint, 3DES por ejemplo.

IKEv2 Mensajes de negociación

Mensaje	Explicación
AWS solicitud procesada por túnel (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la solicitud CREATE_CHILD_SA de CGW.
AWS tunnel está enviando una respuesta (id=xxx) para CREATE_CHILD_SA	AWS está enviando la respuesta CREATE_CHILD_SA a CGW.
AWS tunnel está enviando una solicitud (id=xxx) para CREATE_CHILD_SA	AWS está enviando la solicitud CREATE_CHILD_SA a CGW.
AWS respuesta procesada por túnel (id=xxx) para CREATE_CHILD_SA	AWS ha recibido la respuesta CREATE_CHILD_SA de CGW.

Mensajes de estado del BGP

Los mensajes de estado de BGP contienen información relacionada con las transiciones de estado de la sesión de BGP, las advertencias de límite de prefijos, las infracciones de los límites, las notificaciones de sesión de BGP, los mensajes de BGP OPEN y las actualizaciones de atributos de un BGP vecino para una sesión de BGP determinada.

Mensaje	Estado de BGP	Explicación
El estado de la sesión BGP homóloga del lado de AWS ha cambiado de Inactivo a Connect with neighbor {ip: xxx}	ABAJO	El estado de la conexión BGP en AWS se ha actualizado a Connect.
El estado de la sesión BGP homóloga del lado de AWS ha cambiado de Connect a OpenSent with neighbor {ip: xxx}	ABAJO	El estado de la conexión BGP en el lado de AWS se ha actualizado a OpenSent.
El estado de la sesión BGP homóloga del lado de AWS ha cambiado de OpenSent a OpenConfirm con el vecino {ip: xxx}	ABAJO	El estado de la conexión BGP en el lado de AWS se ha actualizado a OpenConfirm.
El estado de la sesión BGP homóloga del lado de AWS ha cambiado de OpenConfirm a Establecido con el vecino {ip: xxx}	ARRIBA	El estado de la conexión BGP en el lado de AWS se actualizó a Established.
El estado de la sesión BGP homóloga del lado de AWS ha cambiado de establecido a inactivo con el vecino {ip: xxx}	ABAJO	El estado de la conexión BGP en el lado de AWS se ha actualizado a inactivo.
El estado de la sesión BGP homóloga del lado de AWS ha cambiado de Connect a Active with neighbor {ip: xxx}	ABAJO	El estado de la conexión BGP en el lado de AWS pasó de Connect a Active. Compruebe la disponibilidad del puerto TCP 179 en CGW si la sesión

Mensaje	Estado de BGP	Explicación
		BGP está bloqueada en el estado Connect.
El par de AWS informa de una advertencia de límite máximo de prefijos: recibió {prefijos (count): xxx} prefijos del vecino {ip: xxx}, el límite es {limit (numérico): xxx}	ARRIBA	La parte de AWS genera periódicamente un mensaje de registro cuando el número de prefijos recibidos de la CGW se acerca al límite permitido.
El par de AWS detectó que se había superado el límite máximo de prefijos: recibió {prefijos (recuento): xxx} prefijos del vecino {ip: xxx}, el límite es {límite (numérico): xxx}	ABAJO	La parte de AWS genera un mensaje de registro cuando la cantidad de prefijos recibidos de la CGW supera el límite permitido.
Un compañero de AWS envió una notificación 6/1 (cesar/al canzar el número máximo de prefijos) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par BGP de CGW para indicar que la sesión de BGP había finalizado o debido a una infracción del límite de prefijos.
El compañero de AWS recibió la notificación 6/1 (cesar/al canzar el número máximo de prefijos) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par de CGW en la que se indicaba que la sesión de BGP había finalizado o debido a una infracción del límite de prefijos.

Mensaje	Estado de BGP	Explicación
Un compañero del lado de AWS envió una notificación 6/2 (ceso/cierre administrativo) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par BGP de CGW para indicar que la sesión de BGP había finalizado.
Un compañero del lado de AWS recibió la notificación 6/2 (cese o cierre administrativo) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par de CGW para indicar que la sesión de BGP había finalizado.
Un compañero del lado de AWS envió una notificación 6/3 (Cease/Peer sin configuración) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par de CGW para indicar que el par no está configurado o se ha eliminado de la configuración.
El compañero del lado de AWS recibió la notificación 6/3 (Cease/Peer sin configurar) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par de CGW para indicar que el par no está configurado o se ha eliminado de la configuración.
Un compañero del lado de AWS envió una notificación 6/4 (ceso/restablecimiento administrativo) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par BGP de CGW para indicar que se había restablecido la sesión de BGP.
Un compañero de AWS recibió la notificación 6/4 (ceso/restablecimiento administrativo) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par de CGW para indicar que la sesión de BGP se había restablecido.

Mensaje	Estado de BGP	Explicación
Un compañero del lado de AWS envió una notificación el 6 de mayo (cese o conexión rechazada) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par BGP de CGW para indicar que se había rechazado la sesión de BGP.
El compañero de AWS recibió la notificación 6/5 (cesar/co nexión rechazada) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par de CGW en la que se indicaba que la sesión de BGP había sido rechazada.
Un compañero del lado de AWS envió una notificación 6/6 (cesar/otro cambio de configuración) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par BGP de CGW para indicar que se había producido un cambio en la configuración de la sesión de BGP.
El compañero de AWS recibió la notificación 6/6 (cesar/otro cambio de configuración) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par CGW que indica que se ha producido un cambio en la configuración de la sesión de BGP.
Un compañero del lado de AWS envió una notificación 6/7 (resolución de ceso/colisión de conexión) al vecino {ip: xxx}	ABAJO	La parte de AWS envió una notificación al par de CGW para resolver una colisión de conexión cuando ambos pares intentaban establecer una conexión simultáneamente.

Mensaje	Estado de BGP	Explicación
Un compañero del lado de AWS recibió la notificación 6/7 (resolución de ceso/colisión de conexión) del vecino {ip: xxx}	ABAJO	La parte de AWS recibió una notificación del par CGW en la que se indicaba la resolución de una colisión de conexión cuando ambos pares intentaban establecer una conexión simultáneamente.
Un compañero de AWS envió una notificación de caducidad del temporizador de espera al vecino {ip: xxx}	ABAJO	El temporizador de espera del BGP expiró y la parte de AWS envió una notificación a la CGW.
Un par del lado de AWS detectó un mensaje OPEN incorrecto del vecino {ip: xxx}; el AS remoto es {asn: xxx}, se esperaba {asn: xxx}	ABAJO	La parte de AWS detectó que se había recibido un mensaje OPEN incorrecto del par CGW, lo que indica una discordancia de configuración.
Un compañero de AWS recibió un mensaje OPEN del vecino {ip: xxx}: versión 4, AS {asn: xxx}, holdtime {holdtime (seconds): xxx}, router-id {id: xxx}}	ABAJO	La parte de AWS recibió un mensaje de apertura de BGP para iniciar una sesión de BGP con el par de CGW.
Un compañero de AWS envió un mensaje OPEN al vecino {ip: xxx}: versión 4, AS {asn: xxx}, holdtime {holdtime (seconds): xxx}, router-id {id: xxx}	ABAJO	El par de CGW envió un mensaje de apertura de BGP para iniciar una sesión de BGP con el par de BGP del lado de AWS.

Mensaje	Estado de BGP	Explicación
El par del lado de AWS está iniciando una conexión (a través de Connect) con el vecino {ip: xxx}	ABAJO	La parte de AWS está intentando conectarse con el vecino BGP de CGW.
Un compañero de AWS envió un End-of-RIB mensaje a su vecino {ip: xxx}	ARRIBA	La parte de AWS ha terminado de transmitir las rutas a la CGW tras el establecimiento de la sesión de BGP.
El compañero de AWS recibió una actualización con los atributos del vecino {ip: xxx} - AS path: {aspath (list): xxx xxx xxx}	ARRIBA	La parte de AWS recibió una actualización de los atributos de sesión de BGP del vecino.

Mensajes de estado de la ruta

A diferencia de los mensajes de estado del BGP, los mensajes de estado de la ruta contienen datos sobre los atributos del BGP de un prefijo determinado, como la ruta AS, la preferencia local, el discriminador de salidas múltiples (MED), la dirección IP del siguiente salto y el peso. Un mensaje de estado de la ruta solo incluirá un campo de detalles cuando haya un error en una ruta que se anunció, actualizó o retiró. Algunos ejemplos son los siguientes

Mensaje	Explicación
DENEGADO debido a: as-path contiene nuestro propio AS	AWS denegó los mensajes de actualización de BGP para un nuevo prefijo de CGW debido a que la ruta contenía el AS propio de los pares del lado de AWS.
DENEGADO debido a: el siguiente salto no está conectado	AWS rechazó un anuncio de ruta BGP para el prefijo de la CGW debido a un error de validación del siguiente salto no conectado.

Mensaje	Explicación
	Asegúrese de que se pueda acceder a la ruta por el lado de la CGW.

Ejemplo de formato de registro para los registros BGP de Tunnel

```
{
  "resource_id": "vpn-1234abcd_1.2.3.4",
  "event_timestamp": 1762580429641,
  "timestamp": "2025-11-08 05:40:29.641Z",
  "type": "BGPStatus",
  "status": "UP",
  "message": {
    "details": "AWS-side peer BGP session state has changed from OpenConfirm to Established with neighbor 169.254.50.85"
  }
}

{
  "resource_id": "vpn-1234abcd_1.2.3.4",
  "event_timestamp": 1762579573243,
  "timestamp": "2025-11-08 05:26:13.243Z",
  "type": "RouteStatus",
  "status": "UPDATED",
  "message": {
    "prefix": "172.31.0.0/16",
    "asPath": "64512",
    "localPref": 100,
    "med": 100,
    "nextHopIp": "169.254.50.85",
    "weight": 32768,
    "details": "DENIED due to: as-path contains our own AS"
  }
}
```

Requisitos de IAM para publicar en los registros CloudWatch

Para que la característica de registro funcione correctamente, la política de IAM asociada a la entidad principal de IAM que se está utilizando para configurar la característica debe incluir los siguientes permisos como mínimo. También puedes encontrar más información en la sección [Habilitar el registro desde determinados AWS servicios](#) de la Guía del usuario de Amazon CloudWatch Logs.

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"
    }
  ]
}
```

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

Vea el registro de actividad de una conexión Site-to-Site VPN. Aquí puede ver los detalles sobre la configuración, como los algoritmos de cifrado o si los registros de VPN de túnel están habilitados. También puede ver el estado del túnel. Esto le ayuda a realizar un mejor seguimiento de cualquier problema o conflicto que pueda tener con una conexión de VPN.

Para consultar la configuración actual de registro de túnel

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN que desea ver en la lista VPN connections (Conexiones de VPN).
4. Elija la pestaña Tunnel details (Detalles de túnel).
5. Amplíe las secciones Tunnel 1 options (Opciones de túnel 1) y Tunnel 2 options (Opciones de túnel 2) para ver todos los detalles de configuración de los túneles.
6. Puede ver el estado actual de la función de registro de VPN de túnel y el grupo de CloudWatch registros actualmente configurado (si lo hay) en el grupo de registros para el CloudWatch registro de VPN de túnel y el formato de salida del registro en Formato de salida para el registro de VPN de túnel.
7. Puede ver el estado actual de la función de registro BGP de túnel y el grupo de CloudWatch registros actualmente configurado (si lo hubiera) en el grupo de registros del CloudWatch registro de VPN de túnel y el formato de salida del registro en Formato de salida para el registro BGP de túnel.

Para ver la configuración actual del registro de túneles en una conexión Site-to-Site VPN mediante la línea de AWS comandos o la API

- [DescribeVpnConnections](#) (API de consultas de Amazon EC2)
- [describe-vpn-connections](#) (AWS CLI)

Habilitar los registros AWS Site-to-Site VPN

Habilite Site-to-Site los registros de VPN para registrar la actividad de la VPN, como el estado del túnel y otros detalles. Puede habilitar el registro en una conexión nueva o modificar una conexión

existente para iniciar el registro de la actividad. Si desea desactivar el registro de una conexión, consulte [Deshabilite los registros de Site-to-Site VPN](#).

 Note

Al habilitar los registros de Site-to-Site VPN para un túnel de conexión VPN existente, la conectividad a través de ese túnel puede interrumpirse durante varios minutos. Sin embargo, cada conexión de VPN ofrece dos túneles para una alta disponibilidad, por lo que puede habilitar el registro en un túnel a la vez mientras mantiene la conectividad a través del túnel que no se modifica. Para obtener más información, consulte [AWS Site-to-Site VPN reemplazos de puntos finales de túneles](#).

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

Siga el procedimiento indicado en [Paso 5: Crear una conexión de VPN](#). En las Tunnel Options (Opciones de túnel) del Paso 9, puede especificar todas las opciones que desea usar para ambos túneles, como las opciones de VPN logging (Registro de VPN). Para obtener más información sobre estas opciones, consulte [Opciones de túnel para su AWS Site-to-Site VPN conexión](#).

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

- [CreateVpnConnection](#) (API de consultas de Amazon EC2)
- [create-vpn-connection](#) (AWS CLI)

Para habilitar el registro de la actividad del túnel en una Site-to-Site conexión VPN existente

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, selecciona conexiones Site-to-Site VPN.
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).
6. En Tunnel activity log (Registro de actividad de túnel), seleccione Enable (Habilitar).

7. En Grupo de CloudWatch registros de Amazon, selecciona el grupo de CloudWatch registros de Amazon al que quieres que se envíen los registros.
8. (Opcional) En Output format (Formato de salida), elija el formato deseado para la salida del registro, ya sea json o text (texto).
9. Seleccione Save changes (Guardar cambios).
10. (Opcional) Repita los pasos 4 a 9 para el otro túnel si lo desea.

Para habilitar el registro BGP de túnel en una Site-to-Site conexión VPN existente

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija conexiones Site-to-Site VPN.
3. Seleccione la conexión 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 el registro BGP de Tunnel, selecciona Activar.
7. En Grupo de CloudWatch registros de Amazon, selecciona el grupo de CloudWatch registros de Amazon al que quieres que se envíen los registros.
8. (Opcional) En Output format (Formato de salida), elija el formato deseado para la salida del registro, ya sea json o text (texto).
9. Seleccione Save changes (Guardar cambios).
10. (Opcional) Repita los pasos 4 a 9 para el otro túnel si lo desea.

Para habilitar el registro de túneles en una conexión Site-to-Site VPN existente mediante la línea de AWS comandos o la API

- [ModifyVpnTunnelOptions](#)(API de consultas de Amazon EC2)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Inhabilitar AWS Site-to-Site VPN los registros

Desactive el registro de VPN en una conexión si ya no quiere seguir rastreando ninguna actividad en esa conexión. Esta acción solo desactiva el registro y no afecta a ninguna otra cosa de esa conexión.

Para habilitar o volver a habilitar el registro en una conexión, consulte [Habilite los registros de Site-to-Site VPN](#).

Para deshabilitar el registro de la actividad del túnel en una conexión Site-to-Site VPN

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Site-to-Site VPN Connections.
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).
6. En Tunnel activity log (Registro de actividad de túnel), desactive Enable (Habilitar).
7. Seleccione Save changes (Guardar cambios).
8. (Opcional) Repita los pasos 4 a 7 para el otro túnel si lo desea.

Para deshabilitar el registro BGP de túnel en una Site-to-Site conexión VPN

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Site-to-Site VPN Connections.
3. Seleccione la conexión de VPN que desea modificar de la lista VPN connections (Conexiones de VPN).
4. Seleccione Actions (Acciones), Modify VPN tunnel options (Modificar opciones de túnel de VPN).
5. Seleccione el túnel que desea modificar; para ello, elija la dirección IP adecuada en la lista VPN tunnel outside IP address (Túnel de VPN fuera de la dirección IP).
6. En el registro BGP del túnel, desactive Activar.
7. Seleccione Save changes (Guardar cambios).
8. (Opcional) Repita los pasos 4 a 7 para el otro túnel si lo desea.

Para deshabilitar el registro de túneles en una conexión Site-to-Site VPN mediante la línea de AWS comandos o la API

- [ModifyVpnTunnelOptions](#)(API de consultas de Amazon EC2)
- [modify-vpn-tunnel-options](#) (AWS CLI)

Supervise AWS Site-to-Site VPN los túneles con Amazon CloudWatch

Puede monitorizar los túneles de la VPN mediante CloudWatch el cual se recopilan y procesan los datos sin procesar del servicio VPN para convertirlos en métricas legibles y prácticamente en tiempo real. Estas estadísticas se registran durante un periodo de 15 meses, de forma que pueda obtener acceso a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio. Los datos de las métricas de la VPN se envían automáticamente a CloudWatch medida que están disponibles.

Para obtener más información, consulta la [Guía del CloudWatch usuario de Amazon](#).

Contenido

- [Dimensiones y métricas de VPN](#)
- [Ver las métricas CloudWatch de Amazon Logs para AWS Site-to-Site VPN](#)
- [Crea CloudWatch alarmas de Amazon para monitorear AWS Site-to-Site VPN los túneles](#)

Dimensiones y métricas de VPN

Las siguientes CloudWatch métricas están disponibles para sus conexiones Site-to-Site VPN.

Métrica	Descripción
TunnelState	El estado de los túneles. Para la estática VPNs, 0 indica ABAJO y 1 indica ARRIBA. Para BGP VPNs, 1 indica ESTABLECIDO y 0 se usa para todos los demás estados. Para ambos tipos de VPNs, los valores entre 0 y 1 indican que al menos un túnel no está ACTIVO. Unidades: valor fraccional entre 0 y 1
TunnelDataIn †	Los bytes recibidos en el AWS lateral de la conexión a través del túnel VPN desde una pasarela de cliente. Cada punto de datos de la métrica representa el número de bytes

Métrica	Descripción
	recibidos después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes recibidos durante el periodo. Esta métrica cuenta los datos después del descifrado. Unidades: bytes
TunnelDataOut †	Los bytes enviados desde el AWS lado de la conexión a través del túnel VPN hasta la pasarela del cliente. Cada punto de datos de la métrica representa el número de bytes enviados después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes enviados durante el periodo. Esta métrica cuenta los datos antes del cifrado. Unidades: bytes
ConcentratorBandwidthUsage	El uso del ancho de banda para una conexión de Site-to-Site VPN Concentrator. Esta métrica está disponible para las conexiones VPN que utilizan un concentrador Site-to-Site VPN. Use la estadística promedio para mostrar el uso promedio de ancho de banda durante el período. Unidades: bits por segundo

† 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	Description (Descripción)
VpnId	Filtra los datos de las métricas por el ID de conexión Site-to-Site VPN.
TunnelIpAddress	Filtra los datos de las métricas en función de la dirección IP del túnel de la gateway privada virtual.

Ver las métricas CloudWatch de Amazon Logs para AWS Site-to-Site VPN

Cuando creas una conexión Site-to-Site VPN, el servicio VPN envía métricas sobre tu conexión VPN a CloudWatch medida que están disponibles. Puede ver las métricas de la conexión de VPN de la siguiente manera.

Para ver las métricas mediante la CloudWatch consola

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, seleccione Métricas.
3. En All metrics elija el espacio de nombres de métricas VPN.
4. Seleccione la dimensión de métrica para ver las métricas, por ejemplo, Métricas de túneles de VPN.

Note

El espacio de nombres de la VPN no aparecerá en la CloudWatch consola hasta que se haya creado una conexión Site-to-Site VPN en la AWS región que está viendo.

Para ver las métricas mediante el AWS CLI

En el símbolo del sistema, ejecute el siguiente comando:

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

Crea CloudWatch alarmas de Amazon para monitorear AWS Site-to-Site VPN los túneles

Puede crear una CloudWatch alarma que envíe un mensaje de Amazon SNS cuando la alarma cambie de estado. Una alarma vigila una única métrica durante el período especificado y envía una notificación a un tema de Amazon SNS según el valor de la métrica relativo a un determinado umbral durante varios períodos de tiempo.

Por ejemplo, puede crear una alarma que monitoree el estado de un único túnel de VPN y envíe una notificación cuando el estado del túnel sea INACTIVO durante 3 puntos de datos en 15 minutos.

Para crear una alarma para el estado de un único túnel

1. Abra la CloudWatch consola en. <https://console.aws.amazon.com/cloudwatch/>
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Elija VPN y, a continuación, elija Métricas de túnel de VPN.
5. Seleccione la dirección IP del túnel deseado, en la misma línea que la TunnelState métrica. Elija Seleccionar métrica.
6. Para siempre que TunnelState sea... , seleccione Inferior y, a continuación, introduzca «1" en el campo de entrada situado debajo de... .
7. En Configuración adicional, establezca las entradas en "3 de 3" para los Puntos de datos para la alarma.
8. Elija 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. Elija Siguiente.
12. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Puede crear una alarma que supervise el estado de la conexión Site-to-Site VPN. Por ejemplo, puede crear una alarma que envíe una notificación cuando el estado de uno o ambos túneles esté INACTIVO durante un período de 5 minutos.

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

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Elija VPN y, a continuación, elija VPN Connection Metrics (Métricas de conexión VPN).
5. Seleccione su conexión Site-to-Site VPN y la TunnelState métrica. Elija Select metric (Seleccionar métrica).
6. En Statistic (Estadística), especifique Maximum (Máximo).

Como alternativa, si has configurado tu conexión Site-to-Site VPN para que ambos túneles estén activos, puedes especificar una estadística de Mínimo para enviar una notificación cuando al menos un túnel esté inactivo.

7. En Siempre, elija Menor o igual que ($\leq$) e introduzca 0 (o 0,5 cuando hay al menos un túnel desactivado). Elija Siguiente.
8. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Siguiente.
9. Escriba un nombre y la descripción de su alarma. Elija 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 CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Seleccione VPN y, a continuación, elija VPN Tunnel Metrics (Métricas de túnel de VPN).
5. Seleccione la dirección IP del túnel VPN y la TunnelDataIn métrica. 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)($\geq$) y escriba 5000000. Elija Siguiente.
9. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Siguiente.
10. Escriba un nombre y la descripción de su alarma. Elija Siguiente.
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

La siguiente alarma monitoriza la cantidad de tráfico que sale del túnel de VPN a su red, y envía una notificación cuando el número de bytes sea inferior a 1 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red saliente

1. Abra la CloudWatch consola en <https://console.aws.amazon.com/cloudwatch/>.
2. En el panel de navegación, amplíe Alarmas y, a continuación, elija Todas las alarmas.
3. Elija Crear alarma y, a continuación, elija Seleccionar métrica.
4. Seleccione VPN y, a continuación, elija VPN Tunnel Metrics (Métricas de túnel de VPN).
5. Seleccione la dirección IP del túnel VPN y la TunnelDataOut métrica. 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)($\leq$) y escriba 1000000. Elija Siguiente.
9. En Select an SNS topic (Seleccionar un tema de SNS), seleccione una notificación existente o elija New list (Nueva lista) para crear una. Elija Siguiente.
10. Escriba un nombre y la descripción de su alarma. Elija Siguiente.
11. Compruebe la configuración de la alarma y, a continuación, elija Create alarm (Crear alarma).

Para ver más ejemplos de creación de alarmas, consulta [Cómo crear CloudWatch alarmas de Amazon](#) en la Guía del CloudWatch usuario de Amazon.

AWS Health y AWS Site-to-Site VPN eventos

AWS Site-to-Site VPN envía automáticamente notificaciones a [Panel de estado](#). Este panel no requiere configuración y está listo para ser utilizado por AWS los usuarios autenticados. Puede configurar varias acciones en respuesta a las notificaciones de eventos a través de Panel de estado.

Panel de estado Proporciona los siguientes tipos de notificaciones para sus conexiones VPN:

- [Notificaciones de sustitución de puntos de enlace de un túnel](#)
- [Notificaciones de VPN con un solo túnel](#)

Notificaciones de sustitución de puntos de enlace de un túnel

Recibirá una notificación de sustitución del punto final del túnel Panel de estado cuando se sustituya uno o ambos puntos finales del túnel VPN de su conexión VPN. El punto de enlace de un túnel se reemplaza cuando AWS realiza actualizaciones en el túnel o cuando se modifica su conexión de VPN. Para obtener más información, consulte [AWS Site-to-Site VPN reemplazos de puntos finales de túneles](#).

Cuando se completa el reemplazo del punto final del túnel, AWS envía la notificación de reemplazo del punto final del túnel a través de un Panel de estado evento.

Notificaciones de VPN con un solo túnel

Una conexión Site-to-Site VPN consta de dos túneles para garantizar la redundancia. Se recomienda encarecidamente que configure ambos túneles para disfrutar de una alta disponibilidad. Si la conexión VPN tiene un único túnel activo y el otro se mantiene inactivo durante más de una hora al día, recibirá una notificación de túnel de VPN único mensual a través de un evento de Panel de estado . Este evento se actualizará diariamente con cualquier conexión VPN nueva detectada como túnel único, y las notificaciones se enviarán semanalmente. Cada mes se creará un nuevo evento que borrará todas las conexiones de VPN que ya no se detecten como túnel único.

AWS Site-to-Site VPN cuotas

Su AWS cuenta tiene las siguientes cuotas, anteriormente denominadas límites, relacionadas con la Site-to-Site VPN. A menos que se indique lo contrario, cada cuota es específica de la región de . Puede solicitar el aumento de algunas cuotas, pero otras no se pueden aumentar.

Para solicitar un aumento de una cuota ajustable, elija Yes (Sí) en la columna Adjustable (Ajustable). Para obtener más información, consulte [Solicitud de aumento de cuota](#) en la Guía del usuario de Service Quotas.

Site-to-Site Recursos de VPN

Name	Predeterminado	Ajustable
Gateways de cliente por región	50	Sí
Gateways privadas virtuales por región	5	Sí
Site-to-Site Conexiones VPN por región	50	Sí
Site-to-Site Conexiones VPN por puerta de enlace privada virtual	10	Sí
Conexiones Site-to-Site VPN aceleradas por región	10	Sí
Conexiones Site-to-Site VPN no asociadas por región	10	Sí
Conexiones de túnel de gran ancho de banda por región	50	Sí
Site-to-Site Concentradores de VPN por región	50	Sí
Site-to-Site Concentradores VPN por Transit Gateway o WAN en la nube	5	Sí
Sitios remotos por concentrador de Site-to-Site VPN	100	Sí

Note

Tanto las conexiones aceleradas como las no asociadas se incluyen en la cuota total de conexiones Site-to-Site VPN por región.

Puede asociar una gateway privada virtual a una VPC a la vez. Para conectar la misma conexión Site-to-Site VPN a varias VPCs, te recomendamos que consideres la posibilidad de utilizar una pasarela de tránsito en su lugar. Para obtener más información, consulte [Gateways de tránsito](#) en Gateways de tránsito de Amazon VPC.

Site-to-Site Las conexiones VPN en una pasarela de tránsito están sujetas al límite total de adjuntos de la pasarela de tránsito. Para obtener más información, consulte [Cuotas de gateway de tránsito](#).

Rutas

Las fuentes de rutas anunciadas son las rutas de VPC, otras rutas de VPN y las rutas de las interfaces virtuales de 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.

Name	Predeterminado	Ajustable
Rutas dinámicas anunciadas desde un dispositivo de puerta de enlace del cliente a una conexión Site-to-Site VPN en una puerta de enlace privada virtual	100	No
Rutas anunciadas desde una conexión Site-to-Site VPN en una puerta de enlace privada	1 000	No

Name	Predeterminado	Ajustable
virtual a un dispositivo de puerta de enlace de un cliente		
Rutas dinámicas anunciadas desde un dispositivo de puerta de enlace del cliente a una conexión Site-to-Site VPN en una puerta de enlace de tránsito	1 000	No
Rutas anunciadas desde una conexión Site-to-Site VPN en una pasarela de tránsito a un dispositivo de pasarela del cliente	5 000	No
Rutas estáticas desde un dispositivo de puerta de enlace del cliente a una conexión Site-to-Site VPN en una puerta de enlace privada virtual	100	No

Ancho de banda y rendimiento

Hay muchos factores que pueden afectar al ancho de banda obtenido a través de una conexión Site-to-Site VPN, entre los que se incluyen, entre otros, el tamaño del paquete, la combinación de tráfico (TCP/UDP), las políticas de configuración o limitación en las redes intermedias, el clima de Internet y los requisitos específicos de las aplicaciones.

Name	Predeterminado	Ajustable
Ancho de banda máximo por túnel VPN de VPN Concentrator	Hasta 100 Mbps	No
Cantidad máxima de paquetes por segundo (PPS) por túnel VPN de VPN Concentrator	Hasta 10 000	No
Ancho de banda máximo por túnel VPN estándar	Hasta 1,25 Gbps	No
Cantidad máxima de paquetes por segundo (PPS) por túnel VPN estándar	Hasta 140 000	No

Name	Predeterminado	Ajustable
Ancho de banda máximo por túnel VPN de gran ancho de banda	Hasta 5 Gbps	No
Cantidad máxima de paquetes por segundo (PPS) por túnel VPN de gran ancho de banda	Hasta 400 000	No

Para las conexiones Site-to-Site VPN en una puerta de enlace de tránsito, puede usar el ECMP para obtener un mayor ancho de banda de VPN al agregar varios túneles de VPN. Para utilizar ECMP, la conexión de VPN debe estar configurada para el enrutamiento dinámico. ECMP no es compatible con conexiones de VPN que utilizan enrutamiento estático. Para obtener más información, consulte [Gateway de tránsito](#).

Note

IPv6 VPNs admiten los mismos límites de rendimiento (Gbps y PPS), MTU y ruta que. IPv4 VPNs No hay diferencias de rendimiento entre IPv4 las conexiones VPN. IPv6

Unidad de transmisión máxima (MTU).

Site-to-Site La VPN admite una unidad de transmisión máxima (MTU) de 1446 bytes y un tamaño de segmento máximo (MSS) correspondiente de 1406 bytes. Sin embargo, ciertos algoritmos que utilizan encabezados TCP más grandes pueden reducir eficazmente ese valor máximo. Para evitar la fragmentación, le recomendamos que configure la MTU y el MSS en función de los algoritmos seleccionados. Para obtener más información sobre MTU, MSS y los valores óptimos, consulte [Prácticas recomendadas para un AWS Site-to-Site VPN Dispositivo de gateway de cliente](#).

No se admiten tramas gigantes. Para obtener más información, consulta los [marcos Jumbo](#) en la Guía del EC2 usuario de Amazon.

Una conexión Site-to-Site VPN no admite Path MTU Discovery.

Las limitaciones de la MTU se aplican tanto a las conexiones IPv6 VPN como a IPv4 las conexiones.

Recursos de cuotas adicionales

Para obtener información sobre las cuotas relacionadas con las gateways de tránsito, como el número de conexiones de una gateway de tránsito, consulte [Cuotas de las gateways de tránsito](#) en la Guía de gateways de tránsito de Amazon VPC.

Para ampliar las cuotas de VPC, consulte [Cuotas de Amazon VPC](#) en la Guía del usuario de Amazon VPC.

Historial de documentos de la Guía del usuario de Site-to-Site VPN

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

Cambio	Descripción	Fecha
Site-to-Site Concentradores VPN	Site-to-Site Los concentradores VPN proporcionan un centro centralizado para administrar múltiples conexiones VPN con una escalabilidad mejorada y una arquitectura de red simplificada.	15 de noviembre de 2025
Site-to-Site Soporte de VPN para túneles de gran ancho de banda	Site-to-Site La VPN ahora admite un ancho de banda de túnel grande, lo que permite conectar conexiones a una pasarela de tránsito y a una VPN WAN en la nube con un rendimiento de hasta 5 Gbps.	25 de septiembre de 2025
IPv6 soporte para AWS Site-to-Site VPN para el túnel exterior IPs	Site-to-Site La VPN ahora admite IPv6 direcciones para el túnel exterior IPs en las conexiones VPN Transit Gateway y Cloud WAN. Esto permite una IPv6 migración completa con IPv6 direcciones tanto para el túnel IPs exterior como para el paquete interno IPs (IPv6-in-IPv6), así como para el túnel IPv6 exterior IPs	1 de julio de 2025

con el paquete IPv4 interno
IPs (IPv4-in-IPv6).

[Se actualizó la política
AWSVPCS2 SVpn ServiceRolePolicy AWS gestionada](#)

Se agregaron nuevos permisos a la política AWS administrada que permiten a la Site-to-Site VPN administrar el secreto AWS Secrets Manager administrado de la conexión VPN.

27 de mayo de 2025

[Se han actualizado las
opciones de almacenamiento de claves compartidas
previamente](#)

Site-to-Site La VPN ahora permite AWS Secrets Manager almacenar una clave previamente compartida.

27 de mayo de 2025

[Información de VPN clásica
eliminada](#)

Se ha eliminado la información sobre la VPN clásica de la guía.

19 de enero de 2023

[Mensajes de ejemplo de
registro de VPN](#)

Se han añadido registros de muestra para las conexiones Site-to-Site VPN.

9 de diciembre de 2022

[Utilidad de la configuración de descarga actualizada](#)

Site-to-Site Los clientes de VPN pueden generar plantillas de configuración para dispositivos Customer Gateway (CGW) compatibles, lo que facilita la creación de conexiones VPN a AWS ellos. Esta actualización añade compatibilidad con los parámetros de la versión 2 (IKEv2) de Internet Key Exchange para muchos de los dispositivos CGW más populares e incluye dos nuevos APIs : GetVpnConnectionDeviceTypes y. GetVpnConnectionDeviceSampleConfiguration

21 de septiembre de 2021

[Notificaciones de la conexión de VPN](#)

Site-to-Site La VPN envía automáticamente notificaciones sobre su conexión VPN al Panel de estado.

29 de octubre de 2020

[Iniciación de túnel de VPN](#)

Puede configurar sus túneles VPN para que AWS aparezcan los túneles.

27 de agosto de 2020

[Modificar las opciones de conexión de VPN](#)

Puede modificar las opciones de conexión de su conexión Site-to-Site VPN.

27 de agosto de 2020

[Algoritmos de seguridad adicionales](#)

Puede aplicar algoritmos de seguridad adicionales a sus túneles VPN.

14 de agosto de 2020

<u>IPv6 soporte</u>	Sus túneles VPN pueden soportar IPv6 el tráfico dentro de los túneles.	12 de agosto de 2020
<u>AWS Site-to-Site VPN Guías de fusión</u>	Esta versión combina el contenido de la Guía del administrador de AWS Site-to-Site VPN red en esta guía.	31 de marzo de 2020
<u>Conexiones aceleradas AWS Site-to-Site VPN</u>	Puede activar la aceleración de la AWS Site-to-Site VPN conexión.	3 de diciembre de 2019
<u>Modifique las opciones AWS Site-to-Site VPN del túnel</u>	Puede modificar las opciones de un túnel VPN en una AWS Site-to-Site VPN conexión. También puede configurar opciones de túnel adicionales.	29 de agosto de 2019
<u>AWS Private Certificate Authority soporte para certificados privados</u>	Puede utilizar un certificado privado de AWS Private Certificate Authority para autenticar su VPN.	15 de agosto de 2019
<u>Nueva guía de usuario de Site-to-Site VPN</u>	Esta versión separa el contenido AWS Site-to-Site VPN(anteriormente denominado VPN AWS gestionada) de la Guía del usuario de Amazon VPC.	18 de diciembre de 2018
<u>Modificar la gateway de destino</u>	Puede modificar la puerta de enlace de destino de la AWS Site-to-Site VPN conexión.	18 de diciembre de 2018

<u>ASN personalizado</u>	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
<u>Opciones de túnel de VPN</u>	Puede especificar bloques de CIDR de túnel interior y claves compartidas previamente personalizadas para sus túneles de VPN.	3 de octubre de 2017
<u>Métricas de VPN</u>	Puede ver CloudWatch las métricas de sus conexiones VPN.	15 de mayo de 2017
<u>Mejoras de VPN</u>	La conexión de VPN ahora admite la función de cifrado AES de 256 bits, la función de hash SHA-256, NAT traversal y los grupos Diffie-Hellman adicionales durante las fases 1 y 2 de la conexión. Además, podrá utilizar la misma dirección IP de gateway de cliente para cada conexión de VPN que utilice el mismo dispositivo de gateway de cliente.	28 de octubre de 2015

[Conexiones de VPN mediante configuración de direccionamiento estático](#)

Puede crear conexiones IPsec VPN a Amazon VPC mediante configuraciones de enrutamiento estático. Anteriormente, las conexiones de VPN requerían el uso del protocolo de gateway fronteriza (BGP). Ahora admitimos ambos tipos de conexiones y podrá establecer conectividad desde dispositivos que no son compatibles con BGP, incluidos Cisco ASA y Microsoft Windows Server 2008 R2.

13 de septiembre de 2012

[Propagación de ruta automática](#)

Ahora puede configurar la propagación automática de las rutas desde la VPN y AWS Direct Connect los enlaces a las tablas de enrutamiento de la VPC.

13 de septiembre de 2012

[Site-to-Site VPN CloudHub y conexiones VPN redundantes](#)

Puede comunicarse de forma segura de un sitio a otro con y sin VPC. Puede utilizar conexiones de VPN redundantes para proporcionar una conexión tolerante a errores a su VPC.

29 de septiembre de 2011

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.