AWS Site-to-Site VPN

Guía del usuario

AWS Site-to-Site VPN: Guía del usuario

Table of Contents

¿Qué es AWS Site-to-Site VPN?

De manera predeterminada, las instancias que se lanzan en una Amazon VPC no pueden comunicarse con su propia red (remota). No obstante, puede habilitar el acceso a su red remota desde su VPC asociando una gateway privada virtual a la VPC, creando una tabla de ruteo personalizada, y actualizando las reglas del grupo de seguridad y creando una conexión de AWS Site-to-Site VPN (Site-to-Site VPN).

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

Su conexión de Site-to-Site VPN es una AWS Classic VPN o una AWS VPN. Para obtener más información, consulte Categorías de AWS Site-to-Site VPN (p. 2).

> **Important**
>
> Actualmente, no se admite el tráfico IPv6 mediante una conexión de Site-to-Site VPN.

Contenido

Componentes de su Site-to-Site VPN

Las conexiones de Site-to-Site VPN constan de los componentes siguientes. Para obtener más información acerca de los límites de Site-to-Site VPN, consulte Límites de Amazon VPC en la Guía del usuario de Amazon VPC.

Gateway privada virtual

La gateway privada virtual es el concentrador VPN que se encuentra en el extremo de Amazon de la conexión de Site-to-Site VPN. Cree una gateway privada virtual y asóciela a la VPC desde la que desea crear una conexión de Site-to-Site VPN.

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 (64512). No se puede cambiar el ASN una vez que ha creado la gateway privada virtual. Para comprobar el ASN de su gateway privada virtual, consulte sus detalles en la pantalla Virtual Private Gateways (Gateways privadas virtuales) en la consola de Amazon VPC o utilice el comando de la AWS CLI describe-vpn-gateways.

> **Note**
>
> Si crea su gateway privada virtual antes del 30-06-2018, el ASN predeterminado es 17493 en la región Asia Pacífico (Singapur), 10124 en la región Asia Pacífico (Tokio), 9059 en la región UE (Irlanda) y 7224 en todas las demás regiones.

AWS Transit Gateway

Puede modificar la gateway de destino de la conexión de AWS Site-to-Site VPN desde una gateway privada virtual por una gateway de tránsito. Una gateway de tránsito es un centro de tránsito que

puede utilizar para interconectar sus Virtual Private Clouds (VPC) y las redes locales. Para obtener más información, consulte Modificación de una gateway de destino de la conexión de Site-to-Site VPN (p. 22).

Gateway de cliente

La gateway de cliente es un dispositivo físico o aplicación de software en su extremo de la conexión de Site-to-Site VPN.

Para crear una conexión de AWS, debe crear un recurso de gateway de cliente en Site-to-Site VPN, que proporciona información a AWS acerca del dispositivo de gateway de cliente. La siguiente tabla describe la información que necesitará para crear un recurso de gateway de cliente.

Elemento	Descripción
Dirección IP direccionable de Internet (estática) de la interfaz externa de la gateway de cliente.	El valor de dirección IP pública debe ser estático. Si su gateway de cliente se encuentra detrás de un dispositivo de conversión de direcciones de red (NAT) que admite NAT traversal (NAT-T), utilice la dirección IP pública de su dispositivo NAT y ajuste las reglas de su firewall para desbloquear el puerto UDP 4500.
El tipo de direccionamiento: estático o dinámico.	Para obtener más información, consulte Opciones de direccionamiento de Site-to-Site VPN (p. 8).
(Solo direccionamiento dinámico) Número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) de la gateway de cliente.	Puede utilizar un ASN existente asignado a su red. Si no tiene ninguno, puede utilizar un ASN privado (en el intervalo 64512–65534). Si utiliza el asistente para la creación de VPC de la consola para configurar su VPC, se utilizará automáticamente el valor 65000 como ASN.

Para utilizar Amazon VPC con una conexión de Site-to-Site VPN, usted o su administrador de red también deberán configurar la aplicación o el dispositivo de gateway de cliente en su red remota. Cuando se crea la conexión de Site-to-Site VPN, le facilitamos la información de configuración necesaria y el administrador de red normalmente lleva a cabo esta configuración. Para obtener información acerca de la configuración y los requisitos de la gateway de cliente, consulte Su gateway de cliente en la Guía para administradores de red de Amazon VPC.

El túnel de VPN aparece cuando el tráfico se genera desde su lado de la conexión de Site-to-Site VPN. La gateway privada virtual no es el iniciador; su gateway de cliente debe iniciar los túneles. Si su conexión de Site-to-Site VPN registra un periodo de inactividad (de unos 10 segundos, en función de su configuración), es posible que el túnel se ralentice. Para evitar este problema, utilice una herramienta de monitorización de red para generar pings keepalive como, por ejemplo, IP SLA.

Para obtener una lista de gateways de cliente probadas con Amazon VPC, consulte las preguntas frecuentes de Amazon Virtual Private Cloud.

Categorías de AWS Site-to-Site VPN

La conexión de Site-to-Site VPN es una conexión de AWS Classic VPN o una conexión de AWS VPN. Cualquier nueva conexión de Site-to-Site VPN que cree es una conexión de AWS VPN. Las siguientes características solo se admiten en conexiones de VPN AWS:

- Internet Key Exchange versión 2 (IKEv2)
- Recorrido de NAT
- ASN de 4 bytes (además del ASN de 2 bytes)
- Métricas de CloudWatch
- Direcciones IP reutilizables para sus gateways de cliente
- Opciones de cifrado adicionales; incluido el cifrado AES de 256 bits, hash SHA-2 y grupos adicionales Diffie-Hellman
- Opciones de túnel configurables
- ASN privado personalizado para el lado de Amazon de una sesión BGP

Puede averiguar la categoría de su conexión de Site-to-Site VPN utilizando la consola de Amazon VPC o una herramienta de línea de comandos.

Para identificar la categoría de 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 VPN Connections (Conexiones de Site-to-Site VPN).
3. Seleccione la conexión de Site-to-Site VPN y compruebe el valor de Category (Categoría) en el panel de detalles. Un valor de `VPN` indica una conexión AWS VPN. Un valor de `VPN-Classic` indica una conexión AWS Classic VPN.

Para identificar la categoría de Site-to-Site VPN con una herramienta de la línea de comandos

- Puede utilizar el comando de la AWS CLI describe-vpn-connections. En el resultado devuelto, busque y anote el valor de `Category`. Un valor de `VPN` indica una conexión AWS VPN. Un valor de `VPN-Classic` indica una conexión AWS Classic VPN.

  En el siguiente ejemplo, la conexión de Site-to-Site VPN es una conexión de AWS VPN.

```
aws ec2 describe-vpn-connections --vpn-connection-ids vpn-1a2b3c4d
```

```
{
    "VpnConnections": [
        {
            "VpnConnectionId": "vpn-1a2b3c4d",

            ...

            "State": "available",
            "VpnGatewayId": "vgw-11aa22bb",
            "CustomerGatewayId": "cgw-ab12cd34",
            "Type": "ipsec.1",
            "Category": "VPN"
        }
    ]
}
```

También puede usar uno de los siguientes comandos:

- DescribeVpnConnections (API de consulta de Amazon EC2)
- Get-EC2VpnConnection (Herramientas para Windows PowerShell)

Migración de AWS Classic VPN a AWS VPN

Si su conexión de Site-to-Site VPN existente es una conexión AWS Classic VPN, puede migrar a una conexión AWS VPN creando una nueva gateway privada virtual y conexión de Site-to-Site VPN, desasociando la antigua gateway privada virtual de su VPC y asociando la nueva gateway privada virtual a su VPC.

Si su gateway privada virtual existente está asociada a varias conexiones de Site-to-Site VPN, debe volver a crear cada conexión de Site-to-Site VPN para la nueva gateway privada virtual. Si hay varias interfaces virtuales privadas de AWS Direct Connect asociadas a su gateway privada virtual, debe volver a crear cada interfaz virtual privada para la nueva gateway privada virtual. Para obtener más información, consulte Creación de una interfaz virtual en la Guía del usuario de AWS Direct Connect.

Si su conexión de Site-to-Site VPN es una conexión de AWS VPN, no puede migrar a una conexión de AWS Classic VPN.

> **Note**
>
> Durante este procedimiento, la conectividad en la conexión VPC actual se interrumpe al deshabilitar la propagación de rutas y desasociar la gateway privada virtual antigua de su VPC. La conectividad se restaura cuando la nueva gateway privada virtual se asocia a su VPC y la nueva conexión de Site-to-Site VPN está activa. Asegúrese de planificar el tiempo de inactividad previsto.

Para migrar a una conexión AWS VPN

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Virtual Private Gateways (Gateways privadas virtuales), Create Virtual Private Gateway (Crear gateway privada virtual) y cree una gateway privada virtual.
3. En el panel de navegación, elija Site-to-Site VPNConnections (Conexiones de Site-to-Site VPN), Create VPN Connection (Crear conexión de VPN). Especifique la información siguiente y elija Yes, Create (Sí, crear).
   - Virtual Private Gateway (Gateway privada virtual): seleccione la gateway privada virtual que creó en el paso anterior.
   - Customer Gateway (Gateway de cliente): elija Existing (Existente) y seleccione la gateway de cliente existente para su conexión AWS Classic VPN actual.
   - Especifique las opciones de direccionamiento según corresponda.
4. Seleccione la nueva conexión de Site-to-Site VPN y elija Download Configuration (Descargar configuración). Descargue el archivo de configuración adecuado para su dispositivo de gateway de cliente.
5. Utilice el archivo de configuración para configurar túneles de VPN en su dispositivo de gateway de cliente. Para ver ejemplos, consulte Guía para administradores de red de Amazon VPC. No habilite los túneles todavía. Póngase en contacto con su proveedor si necesita asesoramiento para mantener deshabilitados los túneles recién configurados.
6. (Opcional) Cree la VPC de prueba y asocie la gateway privada virtual a la VPC de prueba. Cambie las direcciones de destino origen/dominio de cifrado según corresponda y pruebe la conectividad desde un host en su red local con una instancia de prueba en la VPC de prueba.
7. Si está utilizando la propagación de rutas para su tabla de ruteo, elija Route Tables (Tablas de ruteo) en el panel de navegación. Seleccione la tabla de ruteo para su VPC y elija Route Propagation (Propagación de rutas), Edit (Editar). Desactive la casilla de verificación para la gateway privada virtual antigua y elija Save (Guardar).

   > **Note**
   >
   > A partir de este paso, la conectividad se interrumpe hasta que la nueva gateway privada virtual se asocia y la nueva conexión de Site-to-Site VPN está activa.

8. En el panel de navegación, elija Virtual Private Gateways (Gateways privadas virtuales). Seleccione la antigua gateway privada virtual y elija Actions (Acciones), Detach from VPC (Separar de la VPC), Yes, Detach (Sí, separar). Seleccione la nueva gateway privada virtual y elija Actions (Acciones), Attach to VPC (Asociar a la VPC). Especifique la VPC para su conexión de Site-to-Site VPN y elija Yes, Attach (Sí, asociar).
9. En el panel de navegación, elija Route Tables (Tables de ruteo). Seleccione la tabla de ruteo para su VPC y realice una de las siguientes acciones:
   - Si está utilizando la propagación de rutas, elija Route Propagation (Propagación de rutas), Edit (Editar). Seleccione la nueva gateway privada virtual que ha asociado a la VPC y elija Save (Guardar).
   - Si está utilizando rutas estáticas, elija Routes (Rutas), Edit (Editar). Modifique la ruta para que apunte a la nueva gateway privada virtual y elija Save (Guardar).
10. Habilite los nuevos túneles en su dispositivo de gateway de cliente y deshabilite los túneles antiguos. Para abrir el túnel, debe iniciar la conexión desde su red local.

    Si procede, compruebe su tabla de ruteo para asegurarse de que las rutas se están propagando. Las rutas se propagan a la tabla de ruteo cuando el estado del túnel de VPN es `UP`.

    Note

    Si necesita revertir a su configuración anterior, desasocie la nueva gateway privada virtual y siga los pasos 8 y 9 para volver a asociar a la antigua gateway privada virtual y actualizar las rutas.
11. Si ya no necesita su conexión de AWS Classic VPN y no desea seguir incurriendo en cargos en la misma, quite las configuraciones de túnel anteriores de su dispositivo de gateway de cliente y elimine la conexión de Site-to-Site VPN. Para ello, vaya a Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN), seleccione la conexión de Site-to-Site VPN y elija Delete (Eliminar).

    Important

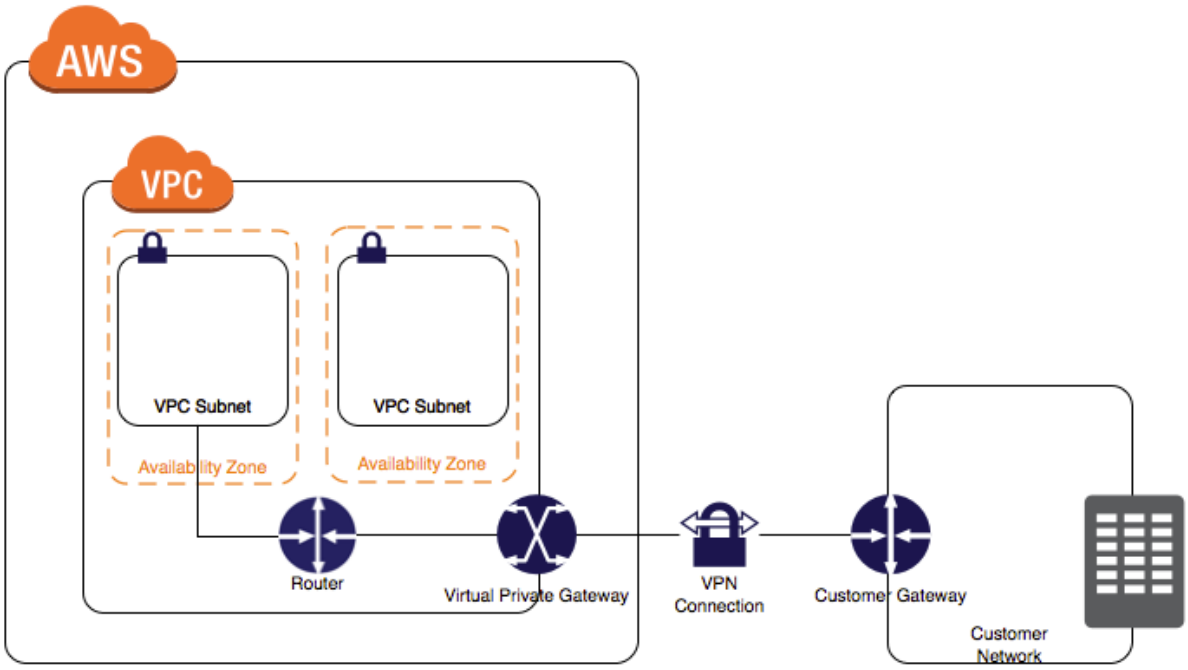
    Después de haber eliminado la conexión AWS Classic VPN, no puede revertir o migrar su conexión de AWS VPN de vuelta a una conexión AWS Classic VPN.

Ejemplos de configuración de Site-to-Site VPN

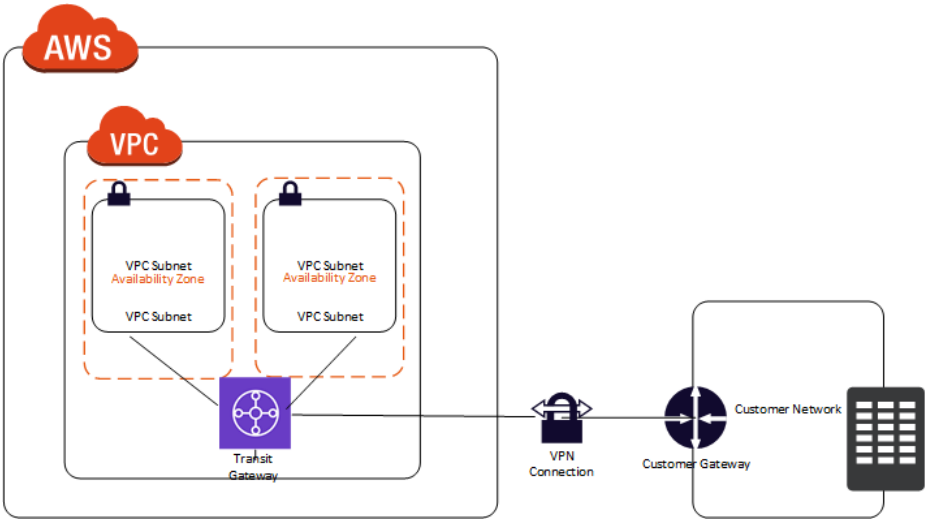
Los diagramas siguientes muestran conexiones de Site-to-Site VPN sencillas y múltiples. La VPC dispone de una gateway privada virtual asociada y su red remota incluye una gateway de cliente que deberá configurar para habilitar la conexión de Site-to-Site VPN. Configure el direccionamiento para que el tráfico procedente de la VPC vinculada a su red se direccione a la gateway privada virtual.

Cuando cree múltiples conexiones de Site-to-Site VPN a una única VPC, podrá configurar una segunda gateway de cliente para que cree una conexión redundante a la misma ubicación externa. También puede utilizarla para crear conexiones de Site-to-Site VPN a varias ubicaciones geográficas.

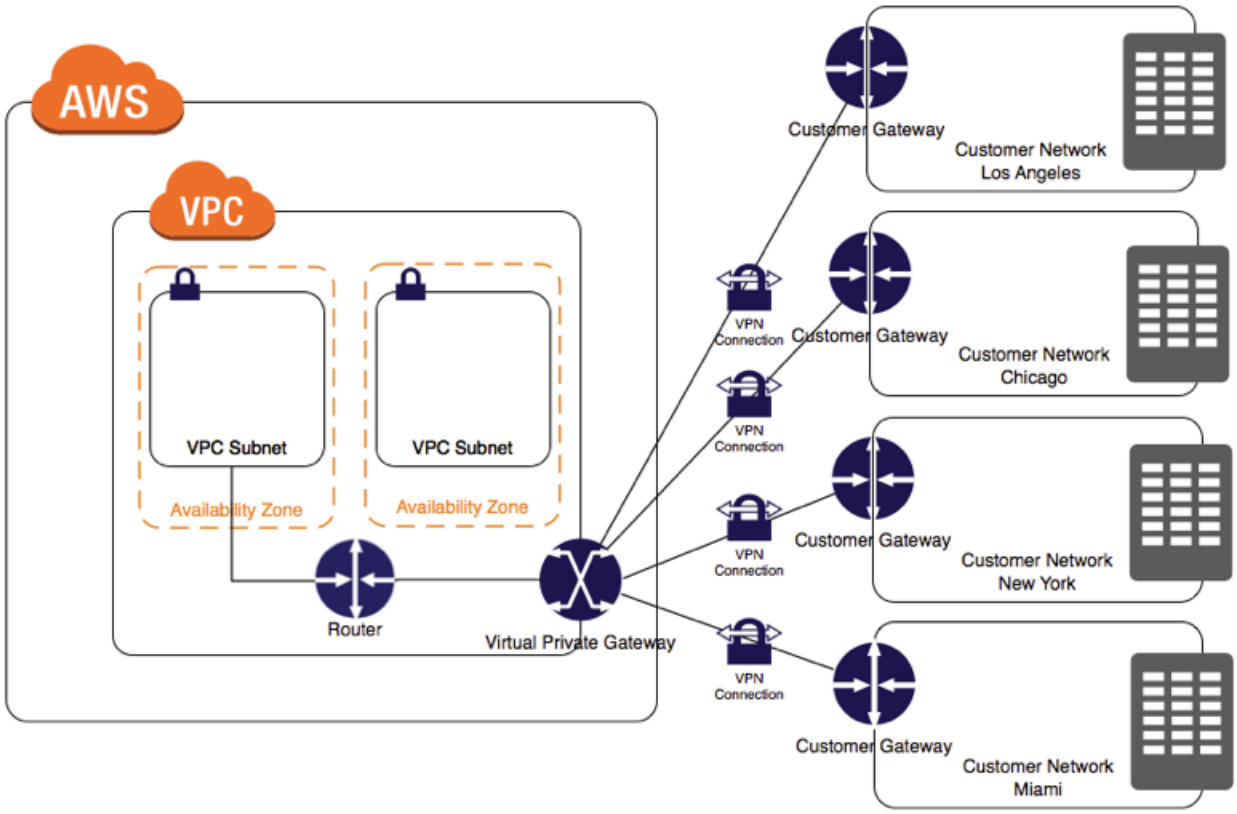
Conexión de Site-to-Site VPN única



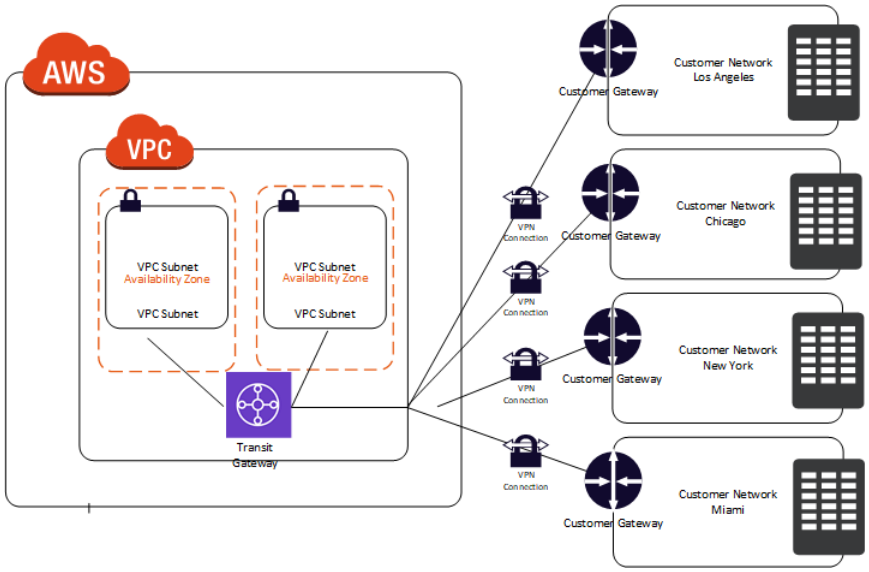
Conexión de Site-to-Site VPN única con una gateway única



Conexiones de Site-to-Site VPN múltiples



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



Opciones de direccionamiento de Site-to-Site VPN

Cuando cree una conexión de Site-to-Site VPN, debe hacer lo siguiente:

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

Existen límites en cuanto al número de rutas que puede añadir a una tabla de ruteo. Para obtener más información, consulte la sección Tablas de ruteo en Límites de Amazon VPC en la Guía del usuario de Amazon VPC.

Direccionamiento estático y dinámico

El tipo de direccionamiento seleccionado puede depender del fabricante y del modelo de sus dispositivos de VPN. Si su dispositivo de VPN admite el protocolo de gateway fronteriza (BGP), especifique el direccionamiento dinámico al configurar la conexión de Site-to-Site VPN. Si su dispositivo no admite BGP, especifique el direccionamiento estático. Para obtener una lista de dispositivos de direccionamiento dinámico probados con Amazon VPC, consulte las preguntas frecuentes de Amazon Virtual Private Cloud.

Cuando utilice un dispositivo BGP, no será necesario especificar ninguna ruta estática a la conexión de Site-to-Site VPN, puesto que el dispositivo utiliza BGP para anunciar sus rutas a la gateway privada virtual. Si utiliza un dispositivo que admite publicidad BGP, no puede especificar rutas estáticas. Si utiliza un dispositivo que no admite BGP, debe seleccionar el direccionamiento estático y escribir las rutas (prefijos IP) de su red que deben comunicarse con 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.

Tablas de ruteo y prioridad de las rutas de VPN

Las tablas de ruteo determinan dónde se dirige el tráfico de red. En la tabla de ruteo, debe añadir 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.

Solo los prefijos IP conocidos para la gateway privada virtual, ya sea mediante anuncios de BGP o por introducción de 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.

Cuando una gateway privada virtual recibe información de direccionamiento, usa la selección de rutas para determinar cómo dirigir el tráfico a su red remota. Se aplica la coincidencia con el prefijo más largo; en caso contrario, se aplican las siguientes reglas:

- En caso de que alguna de las rutas propagadas de una conexión de Site-to-Site VPN o AWS Direct Connect se superpongan con la ruta local de su VPC, se preferirá la ruta local incluso si las rutas propagadas son más específicas.
- Si alguna de las rutas propagadas desde una conexión de Site-to-Site VPN o AWS Direct Connect tiene el mismo bloque de CIDR de destino que otras rutas estáticas (cuando no sea posible aplicar la coincidencia de prefijo más largo), se dará prioridad a las rutas estáticas cuyos objetivos sean puertos

de enlace a Internet, gateways privadas virtuales, interfaces de red, ID de instancia, interconexiones de VPC, gateways NAT o puntos de enlace de la VPC.

Si tiene rutas que se superponen en una conexión de Site-to-Site VPN y no es posible aplicar la coincidencia de prefijo más largo, se dará la prioridad siguiente a las rutas de la conexión de Site-to-Site VPN (ordenadas de mayor a menor preferencia):

- Rutas propagadas de BGP desde una conexión de AWS Direct Connect
- Rutas estáticas añadidas manualmente para una conexión de Site-to-Site VPN
- Rutas propagadas de BGP desde una conexión de Site-to-Site VPN

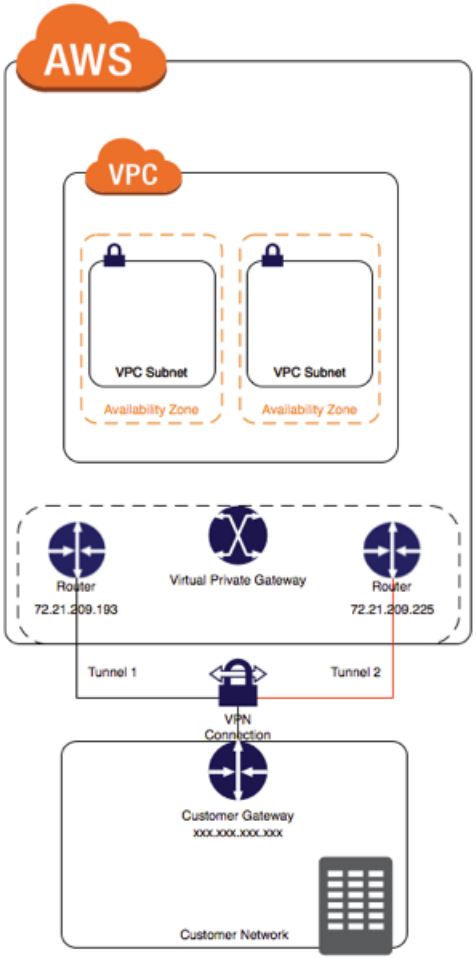
En este ejemplo, la tabla de ruteo tiene una ruta estática a una gateway de Internet (añadida manualmente) y una ruta propagada a una gateway privada virtual. Ambas rutas tienen el destino `172.31.0.0/24`. En este caso, todo el tráfico con destino `172.31.0.0/24` se dirige a la gateway de Internet, ya 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-1a2b3c4d (propagado)
172.31.0.0/24	igw-11aa22bb

Configuración de los túneles de VPN para su conexión de Site-to-Site VPN

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

El siguiente diagrama muestra los dos túneles de la conexión de Site-to-Site VPN.



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

En la siguiente tabla se describen las opciones de túnel que puede configurar.

Elemento	Descripción	Valor predeterminado proporcionado por AWS
CIDR dentro del túnel	El intervalo de direcciones IP internas para el túnel de VPN. Pude especificar un bloque de CIDR de tamaño /30 desde el intervalo `169.254.0.0/16`. El bloque de CIDR debe ser único en todas las conexiones de Site-to-Site VPN que utilizan la misma gateway privada virtual.	Un bloque de CIDR de tamaño /30 desde el intervalo `169.254.0.0/16`.

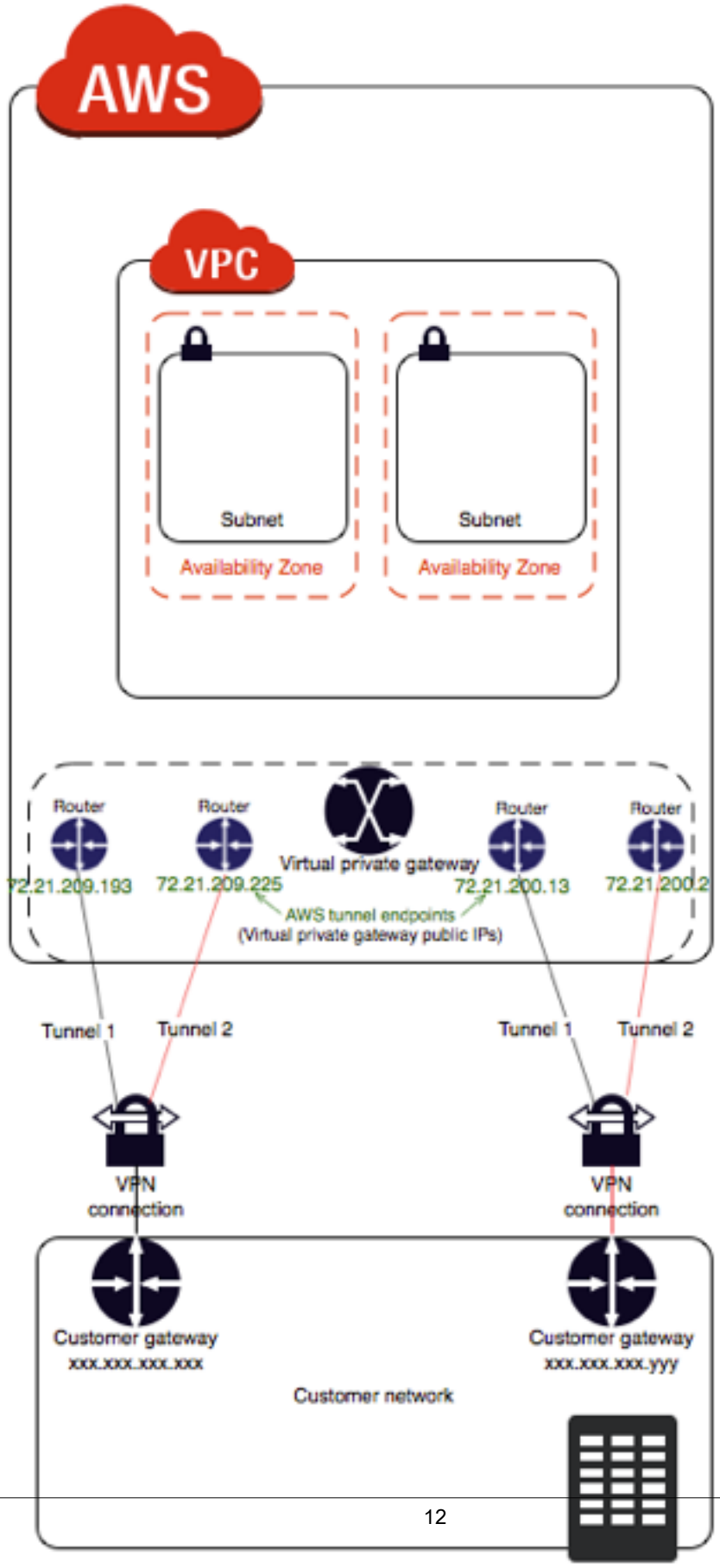
Elemento	Descripción	Valor predeterminado proporcionado por AWS
	Los siguientes bloques de CIDR están reservados y no se pueden utilizar: • `169.254.0.0/30` • `169.254.1.0/30` • `169.254.2.0/30` • `169.254.3.0/30` • `169.254.4.0/30` • `169.254.5.0/30` • `169.254.169.252/30`	
Clave previamente compartida (PSK)	La clave previamente compartida (PSK) para establecer la asociación de seguridad de IKE inicial entre la gateway privada virtual y la gateway 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 (_).	Una cadena alfanumérica de 32 caracteres.

No puede modificar las opciones de túnel después de crear la conexión de Site-to-Site VPN. Para cambiar las direcciones IP de túnel interior o las PSK de una conexión existente, debe eliminar la conexión de Site-to-Site VPN y crear una nueva. No puede configurar las opciones de túnel para una conexión AWS Classic VPN.

Utilización de conexiones de Site-to-Site VPN redundantes para la conmutación por error

Tal como se ha descrito anteriormente, las conexiones de Site-to-Site VPN tienen dos túneles que garantizan la conectividad en caso de que una de las conexiones de Site-to-Site VPN deje de estar disponible. Para ofrecer protección frente a la pérdida de conectividad en caso de que su gateway de cliente deje de estar disponible, puede configurar una segunda conexión de Site-to-Site VPN a su VPC y una gateway privada virtual utilizando una segunda gateway de cliente. La utilización de gateways de cliente y conexiones de Site-to-Site VPN redundantes permite realizar tareas de mantenimiento en una de las gateway de cliente y mantener el flujo de tráfico a través de la segunda gateway de cliente de la conexión de Site-to-Site VPN. Para establecer gateways de cliente y conexiones de Site-to-Site VPN redundantes en su red remota, deberá configurar una segunda conexión de Site-to-Site VPN. La dirección IP de la gateway de cliente de la segunda conexión de Site-to-Site VPN debe estar disponible para el público.

El siguiente diagrama muestra los dos túneles de cada conexión de Site-to-Site VPN y las dos gateways de cliente.


AWS
VPC
Subnet
Availability Zone
Subnet
Availability Zone
Router
Router
Virtual private gateway
Router
Router
72.21.209.193
72.21.209.225
72.21.200.13
72.21.200.2
AWS tunnel endpoints
(Virtual private gateway public IPs)
Tunnel 1
Tunnel 2
Tunnel 1
Tunnel 2
VPN
connection
VPN
connection
Customer gateway
xxx.xxx.xxx.xxx
Customer gateway
xxx.xxx.xxx.yyy
Customer network

Las conexiones de Site-to-Site VPN de direccionamiento dinámico utilizan el protocolo de gateway fronteriza (BGP) para intercambiar la información de direccionamiento entre las gateways de cliente y las gateways privadas virtuales. Las conexiones de Site-to-Site VPN con direccionamiento estático requieren escribir las rutas estáticas de la red remota en su extremo de la gateway de cliente. La información acerca de las rutas que se especifica manualmente y que anuncia mediante BGP permite a las gateways de ambos extremos determinar qué túneles están disponibles para, de este modo, redireccionar el tráfico en caso de error. Por lo tanto, se recomienda configurar su red para que utilice la información de direccionamiento que proporciona BGP (si está disponible) y seleccionar una ruta alternativa. La configuración exacta dependerá de la arquitectura de su red.

Introducción

Utilice los procedimientos siguientes para configurar manualmente la conexión de AWS Site-to-Site VPN. Como opción, puede utilizar el asistente para la creación de VPC para realizar todos estos pasos. Para obtener más información acerca de la utilización del asistente de creación de VPC para configurar la gateway privada virtual, consulte Escenario 3: VPC con subredes públicas y privadas y acceso de AWS Site-to-Site VPN o Escenario 4: VPC solo con una subred privada y acceso AWS Site-to-Site VPN en la Guía del usuario de Amazon VPC.

Siga los pasos que se describen a continuación para configurar una conexión de Site-to-Site VPN:

- Paso 1: Creación de una gateway de cliente (p. 14)
- Paso 2: Creación de una gateway privada virtual (p. 15)
- Paso 3: Habilitación de la propagación de rutas en su tabla de ruteo (p. 15)
- Paso 4: Actualización de su grupo de seguridad (p. 16)
- Paso 5: Creación de una conexión de Site-to-Site VPN y configuración de la gateway de cliente (p. 17)

En este procedimiento se supone que dispone de una VPC con una o varias subredes.

Creación de una gateway de cliente

Una gateway de cliente proporciona información a AWS acerca de su dispositivo de gateway de cliente o aplicación de software. Para obtener más información, consulte Gateway de cliente (p. 2).

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 Customer Gateways (Gateways de cliente) y, a continuación, elija Create Customer Gateway (Crear gateway de cliente).
3. Complete la siguiente información y, a continuación, elija Create Customer Gateway (Crear gateway de cliente):
   - (Opcional) En Name (Nombre), escriba un nombre para su gateway de cliente. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
   - En Routing (Direccionamiento), seleccione el tipo de direccionamiento.
   - Para direccionamiento dinámico, para BGP ASN (ASN de BGP), escriba el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP).
   - En IP Address (Dirección IP), escriba la dirección IP estática direccionable de Internet de su dispositivo de gateway de cliente. Si su gateway de cliente se encuentra detrás de un dispositivo NAT habilitado para NAT-T, utilice la dirección IP pública del dispositivo NAT.

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

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

- New-EC2CustomerGateway (Herramientas de AWS para Windows PowerShell)

Creación de una gateway privada virtual

Al crear una gateway privada virtual, puede especificar opcionalmente el número de sistema autónomo (ASN) privado en el lado de Amazon de la gateway. El ASN debe ser distinto del BGP ASN especificado para la gateway de cliente.

Después de crear una gateway privada virtual, debe asociarla a su VPC.

Para crear una gateway privada virtual y asociarla a su VPC.

1. En el panel de navegación, elija Virtual Private Gateways, Create Virtual Private Gateway.
2. (Opcional) Escriba un nombre para su gateway privada virtual. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
3. En ASN, deje la selección predeterminada para utilizar el ASN de Amazon predeterminado. De lo contrario, elija Custom ASN (ASN predeterminado) y escriba un valor. Para un ASN de 16 bits ASN, el valor debe estar dentro del intervalo de 64512 a 65534. Para un ASN de 32 bits ASN, el valor debe estar dentro del intervalo de 4200000000 a 4294967294.
4. Elija Create Virtual Private Gateway (Crear gateway privada virtual).
5. Seleccione la gateway privada virtual que ha creado y, a continuación, elija Actions (Acciones), Attach to VPC (Asociar a VPC).
6. Seleccione la VPC en la lista y elija Yes, Attach (Sí, asociar).

Para crear una gateway privada virtual mediante la línea de comandos o la API

- CreateVpnGateway (API de consulta de Amazon EC2)
- create-vpn-gateway (AWS CLI)
- New-EC2VpnGateway (Herramientas de AWS para Windows PowerShell)

Para asociar una gateway privada virtual a una VPC mediante la línea de comandos o la API

- AttachVpnGateway (API de consulta de Amazon EC2)
- attach-vpn-gateway (AWS CLI)
- Add-EC2VpnGateway (Herramientas de AWS para Windows PowerShell)

Habilitación de la propagación de rutas en su tabla de ruteo

Para que las instancias de su VPC puedan conectarse con la gateway de cliente, debe configurar su tabla de ruteo para que incluya las rutas que utiliza su conexión de Site-to-Site VPN y hacer que apunten a su gateway privada virtual. Puede habilitar la propagación de rutas para que su tabla de ruteo propague automáticamente dichas rutas a la tabla.

Para el direccionamiento estático, los prefijos de IP estática que especifique en la configuración de su Site-to-Site 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 desde su gateway de cliente se propagarán a la tabla de ruteo cuando el estado de la conexión de Site-to-Site VPN sea `UP`.

Note

Si una conexión se interrumpe, las rutas propagadas en la tabla de ruteo no se retiran automáticamente. Puede ser necesario deshabilitar la propagación de rutas para retirar las rutas propagadas (por ejemplo, si desea que el tráfico conmute por error a una ruta estática).

Para habilitar la propagación de rutas utilizando la consola

1. En el panel de navegación, elija Route Tables (Tablas de ruteo) y, a continuación, seleccione la tabla de ruteo asociada a la subred. De manera predeterminada, esta es la tabla de ruteo principal de la VPC.
2. En la pestaña Route Propagation (Propagación de rutas) del panel de detalles, elija Edit (Editar), seleccione la gateway privada virtual que creó en el procedimiento anterior y, a continuación, elija Save (Guardar).

Note

Para el direccionamiento estático, si no habilita la propagación de rutas, deberá escribir manualmente las rutas estáticas que utiliza su conexión de Site-to-Site VPN. Para ello, seleccione su tabla de ruteo y elija Routes (Rutas), Edit (Editar). En Destination (Destino), añada la ruta estática utilizada por su conexión de Site-to-Site VPN. En Target (Objetivo), seleccione el ID de gateway privada virtual y elija Save (Guardar).

Para deshabilitar la propagación de rutas utilizando la consola

1. En el panel de navegación, elija Route Tables (Tablas de ruteo) y, a continuación, seleccione la tabla de ruteo asociada a la subred.
2. Elija Route Propagation (Propagación de rutas), Edit (Editar). Desactive la casilla de verificación Propagate (Propagar) de la gateway privada virtual y elija Save (Guardar).

Para habilitar la propagación de rutas mediante la línea de comandos o la API

- EnableVgwRoutePropagation (API de consulta de Amazon EC2)
- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (Herramientas de AWS para Windows PowerShell)

Para deshabilitar la propagación de rutas mediante la línea de comandos o la API

- DisableVgwRoutePropagation (API de consulta de Amazon EC2)
- disable-vgw-route-propagation (AWS CLI)
- Disable-EC2VgwRoutePropagation (Herramientas de AWS para Windows PowerShell)

Actualización de su 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 añadir reglas a su grupo de seguridad para habilitar el acceso SSH, RDP e ICMP entrante

1. En el panel de navegación, elija Security Groups (Grupos de seguridad) y, a continuación, seleccione el grupo de seguridad predeterminado para la VPC.
2. En la pestaña Inbound (Entrada) del panel de detalles, añada reglas que permitan el acceso SSH, RDP e ICMP entrante desde su red y, a continuación, elija Save (Guardar). Para obtener más

información acerca de la adición de reglas entrantes, consulte Adición, eliminación y actualización de reglas en la Guía del usuario de Amazon VPC.

Para obtener más información acerca del uso de grupos de seguridad utilizando la AWS CLI, visite Grupos de seguridad de su VPC en la Guía del usuario de Amazon VPC.

Creación de una conexión de Site-to-Site VPN y configuración de la gateway de cliente

Después de crear la conexión de Site-to-Site VPN, descargue la información de configuración y utilícela para configurar el dispositivo de gateway de cliente o la aplicación de software.

Para crear una conexión de Site-to-Site VPN y configurar la gateway de cliente

1. En el panel de navegación, elija Site-to-Site VPNConnections (Conexiones de Site-to-Site VPN), Create VPN Connection (Crear conexión de VPN).
2. Complete la siguiente información y, a continuación, elija Create VPN Connection (Crear conexión de VPN):

   - (Opcional) En Name tag (Etiqueta de nombre), escriba un nombre para su conexión de Site-to-Site VPN. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique.
   - Seleccione la gateway privada virtual que creó anteriormente.
   - Seleccione la gateway de cliente que creó anteriormente.
   - Seleccione una de las opciones de direccionamiento en función de si el router de su VPN admite el protocolo de gateway fronteriza (BGP):
     - Si el router de su VPN admite BGP, elija Dynamic (requires BGP) (Dinámico (requiere BGP)).
     - Si el router de su VPN no admite 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 Site-to-Site VPN.
   - En Tunnel Options (Opciones de túnel), puede especificar opcionalmente la siguiente información para cada túnel:
     - Un bloque de CIDR de tamaño /30 desde el intervalo `169.254.0.0/16` para las direcciones IP de túnel interior.
     - La clave previamente compartida de IKE (PSK). Las siguientes versiones son compatibles: IKEv1 o IKEv2.

     Para obtener más información sobre estas opciones, consulte Configuración de los túneles de VPN para su conexión de Site-to-Site VPN (p. 9).

   La creación de la conexión de Site-to-Site VPN puede tardar unos minutos. Cuando haya finalizado, seleccione la conexión y elija Download Configuration (Descargar configuración).
3. En el cuadro de diálogo Download Configuration (Descargar configuración), seleccione el proveedor, la plataforma y el software que corresponde a su software o dispositivo de gateway de cliente y, a continuación, elija Yes, Download (Sí, descargar).
4. Proporcione el archivo de configuración a su administrador de red junto con la guía siguiente: Guía para administradores de red de Amazon VPC. Cuando el administrador de red haya configurado la gateway de cliente, la conexión de Site-to-Site VPN estará operativa.

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

- CreateVpnConnection (API de consulta de Amazon EC2)

- create-vpn-connection (AWS CLI)
- New-EC2VpnConnection (Herramientas de AWS para Windows PowerShell)

Edición de las reglas estáticas de una conexión de Site-to-Site VPN

Para el direccionamiento estático, puede añadir, modificar o quitar las rutas estáticas de su configuración de VPN.

Para añadir, modificar o quitar una ruta estática

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Elija Static Routes (Rutas estáticas), Edit (Editar).
4. Modifique los prefijos IP estáticos existentes o elija Remove (Eliminar) para eliminarlos. Elija Add Another Rule (Añadir otra regla) para agregar un nuevo prefijo IP a su configuración. Cuando haya terminado, elija Save (Guardar).

   Note

   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 Site-to-Site VPN. Para obtener más información, consulte Habilitación de la propagación de rutas en su tabla de ruteo (p. 15).

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 (Herramientas de AWS para Windows PowerShell)

Para eliminar una ruta estática mediante la línea de comandos o la API

- DeleteVpnConnectionRoute (API de consulta de Amazon EC2)
- delete-vpn-connection-route (AWS CLI)
- Remove-EC2VpnConnectionRoute (Herramientas de AWS para Windows PowerShell)

Sustitución de las credenciales filtradas

Si cree que las credenciales del túnel de su conexión de Site-to-Site VPN se han podido filtrar, cambie la clave de IKE previamente compartida. Para ello, elimine la conexión de Site-to-Site VPN, cree una nueva utilizando la misma gateway privada virtual y configure las nuevas claves en su gateway de cliente. Puede especificar sus claves previamente compartidas al crear la conexión de Site-to-Site VPN. También deberá asegurarse de que las direcciones internas y externas del túnel coincidan, ya que estas pueden cambiarse al volver a crear la conexión de Site-to-Site VPN. Mientras realiza el procedimiento, se detendrá la comunicación con las instancias de la VPC; sin embargo, las instancias seguirán funcionando de manera ininterrumpida. Cuando el administrador de red implemente la nueva información de configuración, la conexión de Site-to-Site VPN utilizará las nuevas credenciales y se reanudará la conexión de red a sus instancias de la VPC.

Important

Este procedimiento requiere la ayuda de su grupo de administradores de redes.

Para cambiar la clave de IKE previamente compartida

1. Elimine la conexión de Site-to-Site VPN. Para obtener más información, consulte Eliminación de una conexión de Site-to-Site VPN (p. 25). No es necesario eliminar la VPC ni la gateway privada virtual.
2. Cree una nueva conexión de Site-to-Site VPN y especifique sus propias claves previamente compartidas para los túneles o deje que AWS genere nuevas claves previamente compartidas para usted. Para obtener más información, consulte Creación de una conexión de Site-to-Site VPN y configuración de la gateway de cliente (p. 17).
3. Descargue el nuevo archivo de configuración.

Comprobación de la conexión de 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. Deberá utilizar una AMI que responda a las solicitudes de ping y necesitará asegurarse de que el grupo de seguridad de su instancia esté configurado para permitir el tráfico ICMP entrante. Se recomienda utilizar una de las AMI de Amazon Linux. Si va a utilizar instancias que ejecuten Windows Server, necesitará iniciar sesión en la instancia y habilitar el tráfico ICMPv4 entrante en el firewall de Windows para poder hacer ping a la instancia.

> **Important**
>
> Debe configurar 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.

Para comprobar la conectividad completa

1. Abra la consola de Amazon EC2 en https://console.aws.amazon.com/ec2/.
2. En el panel, elija Launch Instance (Lanzar instancia).
3. En la página Choose an Amazon Machine Image (AMI) (Elegir una Imagen de máquina de Amazon (AMI)), elija una AMI y, a continuación, elija Select (Seleccionar).
4. Elija un tipo de instancia y, a continuación, elija Next: Configure Instance Details (Siguiente: Configurar detalles de la instancia).
5. En la página Configure Instance Details (Configurar detalles de la instancia), en Network (Red), seleccione su VPC. En Subnet (Subred), seleccione su subred. Elija Next (Siguiente) hasta llegar a la página Configure Security Group (Configurar grupo de seguridad).
6. Seleccione la opción Select an existing security group (Seleccionar un grupo de seguridad existente) y, a continuación, seleccione el grupo predeterminado que modificó antes. Elija Review and Launch (Revisar y lanzar).
7. Revise los ajustes que ha elegido. Realice los cambios que necesite y, a continuación, elija Launch (Lanzar) para seleccionar un par de claves y lanzar la instancia.
8. Cuando la instancia esté en ejecución, obtenga su dirección IP privada (por ejemplo, `10.0.0.4`). La consola de Amazon EC2 muestra la dirección como parte de los detalles de la instancia.
9. Desde un equipo de su red que se encuentre detrás de la gateway de cliente, utilice el comando `ping` con la dirección IP privada de la instancia. La respuesta correcta será similar a la que se muestra a continuación:

```
ping 10.0.0.4
```

```
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
```

Ahora puede utilizar SSH o RDP para conectarse a su instancia en la VPC. Para obtener más información acerca de cómo conectarse a una instancia de Linux, consulte Conexión con la instancia de Linux en la Guía del usuario de Amazon EC2 para instancias de Linux. Para obtener más información acerca de cómo conectarse a una instancia de Windows, consulte Conexión con la instancia de Windows en la Guía del usuario de Amazon EC2 para instancias de Windows.

Modificación de una gateway de destino de la conexión de Site-to-Site VPN

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

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

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

Tareas

- Paso 1: Crear la gateway de tránsito (p. 22)
- Paso 2: Eliminar las rutas estáticas (obligatorio para una conexión de VPN estática al realizar la migración a una gateway de tránsito) (p. 22)
- Paso 3: Migrar a una nueva gateway (p. 23)
- Paso 4: Actualizar tablas de ruteo de VPC (p. 23)
- Paso 5: Actualizar el direccionamiento de la gateway de tránsito (necesario cuando la nueva gateway es una gateway de tránsito) (p. 24)

Paso 1: Crear la gateway de tránsito

Antes de realizar la migración a la nueva gateway, debe configurarla. Para obtener más información acerca de cómo añadir una gateway privada virtual, consulte the section called “Creación de una gateway privada virtual” (p. 15). Para obtener más información acerca de cómo añadir una gateway de tránsito, consulte la sección sobre la creación de la gateway de tránsito en la Gateways de tránsito de Amazon VPC.

Si la nueva gateway de destino es una gateway de tránsito, asocie la VPC a la gateway de tránsito. Para obtener más información acerca de las asociaciones a VPC, consulte la sección sobre asociaciones de gateways en tránsito a una VPC en la Gateways de tránsito de Amazon VPC.

Paso 2: Eliminar las rutas estáticas (obligatorio para una conexión de VPN estática al realizar la migración a una gateway de tránsito)

Este paso es necesario al migrar desde una gateway privada virtual con rutas estáticas a una gateway de tránsito.

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 añadir estas rutas a la gateway de tránsito cuando haya terminado la migración de 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 (Tablas de ruteo) y, a continuación, seleccione la tabla de ruteo.
3. En la pestaña Routes (Rutas), elija Edit (Editar) y, a continuación, elija Remove (Eliminar) en la ruta a la gateway privada virtual.
4. Cuando haya terminado, elija Save (Guardar).

Paso 3: Migrar a una nueva gateway

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Seleccione la conexión de Site-to-Site VPN y elija Actions (Acciones), Modify VPN Connection (Modificar VPN de conexión).
4. En Change Target (Cambiar destino), haga lo siguiente:

   a. En Target Type (Tipo de destino), elija el tipo de gateway .

   b. Configure el destino de la conexión:

      [Gateway privada virtual] En Target VPN Gateway ID (ID de gateway de VPN de destino), elija la gateway privada virtual.

      [Gateway de tránsito] En Target gateway de tránsito ID (ID de gateway de tránsito destino), elija el ID de gateway de tránsito.
5. Seleccione Save (Guardar).

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

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

Paso 4: Actualizar tablas de ruteo de VPC

Después de migrar a la nueva gateway, es posible que tenga que modificar la tabla de ruteo de VPC. En la siguiente tabla se proporciona información sobre las acciones que es necesario realizar. Para obtener información acerca de cómo actualizar las tablas de ruteo de VPC, consulte Tablas de ruteo en la Guía del usuario de Amazon VPC.

Actualizaciones de la tabla de ruteo de VPC necesarias para la modificación del destino de la gateway de VPN

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Gateway privada virtual con rutas propagadas	Gateway de tránsito	Añada una ruta que apunte al ID de gateway de tránsito.

Gateway existente	Nueva gateway	Cambio en la tabla de ruteo de VPC
Gateway privada virtual con rutas propagadas	Gateway privada virtual con rutas propagadas	No se requiere ninguna acción.
Gateway virtual con rutas propagadas	Gateway privada virtual con ruta estática	Añada una entrada que contenga la nueva ID de gateway privada virtual.
Gateway virtual con rutas estáticas	Gateway de tránsito	Actualice la tabla de ruteo de VPC y cambie la entrada que contiene el ID de la gateway privada virtual por el ID de gateway de tránsito.
Gateway virtual con rutas estáticas	Gateway privada virtual con rutas estáticas	Actualice la entrada que apunta al ID de la gateway privada virtual que va a ser el nuevo ID de gateway privada virtual.
Gateway virtual con rutas estáticas	Gateway privada virtual con rutas propagadas	Elimine la entrada que contiene el ID de gateway privada virtual.
Gateway de tránsito	Gateway privada virtual con rutas estáticas	Actualice la entrada que contiene el gateway de tránsito al ID de gateway privada virtual.
Gateway de tránsito	Gateway privada virtual con rutas propagadas	Elimine la entrada que contiene el ID de gateway de tránsito.
Gateway de tránsito	Gateway de tránsito	Actualice la entrada que contiene el ID de gateway de tránsito al nuevo ID de gateway de tránsito .

Paso 5: Actualizar el direccionamiento de la gateway de tránsito (necesario cuando la nueva gateway es una gateway de tránsito)

Cuando la nueva gateway es una gateway de tránsito, modifique la tabla de ruteo de la gateway de tránsito para permitir el tráfico entre la VPC y el Site-to-Site VPN. Para obtener información sobre el direccionamiento de gateway de tránsito, consulte la sección sobre tablas de ruteo de la gateway de tránsito en la Gateways de tránsito de Amazon VPC.

> **Important**
>
> Si ha eliminado rutas estáticas de VPN, debe añadir las rutas estáticas a la tabla de ruteo de gateway de tránsito.

Eliminación de una conexión de Site-to-Site VPN

Si ya no necesita la conexión de AWS Site-to-Site VPN, puede eliminarla.

> **Important**
>
> Si elimina su conexión de Site-to-Site VPN y crea una nueva, tendrá que descargar la nueva información de configuración y necesitará que su administrador de red vuelva a configurar la gateway de cliente.

Para eliminar una conexión de Site-to-Site 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 Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN).
3. Seleccione la conexión de Site-to-Site VPN y elija Actions (Acciones), Delete (Eliminar).
4. Elija Delete (Eliminar).

Si ya no necesita una gateway de cliente, puede eliminarla. No es posible eliminar una gateway de cliente en uso en una conexión de Site-to-Site VPN.

Para eliminar una gateway de cliente con la consola

1. En el panel de navegación, elija Customer Gateways (Gateways de cliente).
2. Seleccione la gateway de cliente que desea eliminar y elija Actions (Acciones), Delete Customer Gateway (Eliminar gateway de cliente).
3. Elija Yes, Delete (Sí, eliminar).

Si ya no necesita una gateway privada virtual para su VPC, puede desvincularla de su VPC.

Para desasociar una gateway privada virtual con la consola

1. En el panel de navegación, elija Virtual Private Gateways (Gateways privadas virtuales).
2. Seleccione la gateway privada virtual y elija Actions (Acciones), Detach from VPC (Desconectar de VPC).
3. Elija Yes, Detach (Sí, desconectar).

Si ya no necesita la gateway privada virtual desconectada, puede eliminarla. Tenga en cuenta que no podrá eliminar la gateway privada virtual si sigue asociada a la VPC.

Para eliminar una gateway privada virtual con la consola

1. En el panel de navegación, elija Virtual Private Gateways (Gateways privadas virtuales).
2. Seleccione la gateway privada virtual que desea eliminar y elija Actions (Acciones), Delete Virtual Private Gateway (Eliminar gateway privada virtual).
3. Elija Yes, Delete (Sí, eliminar).

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

- DeleteVpnConnection (API de consulta de Amazon EC2)
- delete-vpn-connection (AWS CLI)
- Remove-EC2VpnConnection (Herramientas de AWS para Windows PowerShell)

Para eliminar una gateway de cliente mediante la línea de comandos o la API

- DeleteCustomerGateway (API de consulta de Amazon EC2)
- delete-customer-gateway (AWS CLI)
- Remove-EC2CustomerGateway (Herramientas de AWS para Windows PowerShell)

Para desasociar una gateway privada virtual mediante la línea de comandos o la API

- DetachVpnGateway (API de consulta de Amazon EC2)
- detach-vpn-gateway (AWS CLI)
- Dismount-EC2VpnGateway (Herramientas de AWS para Windows PowerShell)

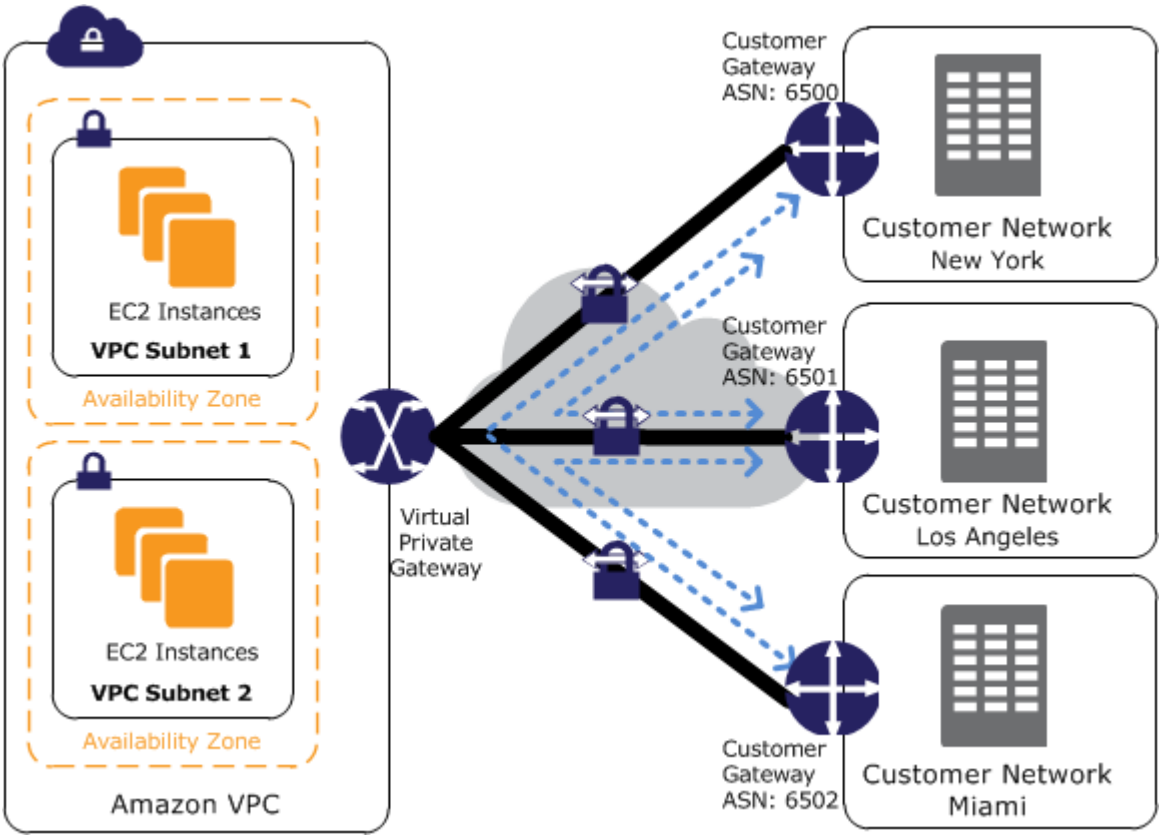
Para eliminar una gateway privada virtual mediante la línea de comandos o la API

- DeleteVpnGateway (API de consulta de Amazon EC2)
- delete-vpn-gateway (AWS CLI)
- Remove-EC2VpnGateway (Herramientas de AWS para Windows PowerShell)

Comunicaciones seguras entre sitios mediante VPN CloudHub

Si tiene varias conexiones de AWS Site-to-Site VPN, puede proporcionar seguridad en la comunicación entre sitios gracias a AWS VPN CloudHub. Esto permite que los sitios remotos puedan comunicarse entre sí y no solo con la VPC. VPN CloudHub funciona con un modelo radial sencillo que puede utilizar con o sin VPC. Este diseño es la opción perfecta para clientes con varias sucursales y conexiones a Internet existentes que desean implementar un modelo radial cómodo y de bajo costo para la conectividad principal o auxiliar entre sus oficinas remotas.

El diagrama siguiente muestra la arquitectura de VPN CloudHub. Las líneas discontinuas azules indican el tráfico de red entre los sitios que se direcciona a través de sus conexiones de Site-to-Site VPN.



Para utilizar AWS VPN CloudHub, debe crear una gateway privada virtual con varias gateways de cliente. Debe utilizar un Número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) único para cada gateway de cliente. Las gateways de cliente anuncian las rutas adecuadas (prefijos de BGP) a través de sus conexiones de Site-to-Site VPN. 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. Los sitios no pueden tener intervalos de IP solapados. Cada sitio puede enviar y recibir datos de la VPC como si estuviese utilizando una conexión de Site-to-Site VPN estándar.

Los sitios que utilizan las conexiones de AWS Direct Connect a la gateway privada virtual también pueden ser parte de AWS VPN CloudHub. Por ejemplo, su sede corporativa de Nueva York puede tener una

conexión de AWS Direct Connect a la VPC y sus sucursales pueden utilizar las conexiones de Site-to-Site VPN a la VPC. De este modo, las sucursales de Los Ángeles y Miami podrán enviar y recibir datos a la sede corporativa y entre ellas mismas gracias a AWS VPN CloudHub.

Para configurar AWS VPN CloudHub, utilice la Consola de administración de AWS para crear varias gateways de cliente, cada una con la dirección IP pública de la gateway y un ASN. A continuación, cree una conexión de Site-to-Site VPN desde cada gateway a una gateway privada virtual común. Cada conexión de Site-to-Site VPN debe anunciar sus rutas de BGP específicas. Esto se realiza utilizando las instrucciones de red de los archivos de configuración de la conexión de Site-to-Site VPN. Las instrucciones de red varían en función del tipo de router que utilice.

Cuando utilice AWS VPN CloudHub, deberá pagar las tasas de conexión de Site-to-Site VPN de Amazon VPC normales. De este modo, se le facturarán las tasas de conexión por cada hora que cada VPN permanezca conectada a la gateway privada virtual. Al enviar datos de un sitio a otro mediante AWS VPN CloudHub, no incurrirá en ningún costo para el envío de datos desde su sitio a la gateway privada virtual. Solo pagará tasas de transferencia de datos de AWS estándar de los datos que se reenvíen desde la gateway privada virtual al punto de enlace. Por ejemplo, si tiene un sitio en Los Ángeles y otro en Nueva York y ambos sitios disponen de una conexión de Site-to-Site VPN a la gateway privada virtual, pagará 0,05 $ por hora por cada conexión de Site-to-Site VPN (un total de 0,10 $ por hora). También pagará las tasas de transferencia de datos de AWS estándar por todos los datos que envíe desde Los Ángeles a Nueva York (y viceversa) que atraviesen cada conexión de Site-to-Site VPN; el tráfico de red enviado a través de la conexión de Site-to-Site VPNa la gateway privada virtual es gratuito, pero el tráfico de red que se envía a través de la conexión de Site-to-Site VPN desde la gateway privada virtual al punto de enlace se facturará según las tasas de transferencia de datos de AWS estándar. Para obtener más información, consulte Precios de las conexiones de Site-to-Site VPN.

Monitorización de la conexión de Site-to-Site VPN

La monitorización es una parte importante del mantenimiento de la fiabilidad, la disponibilidad y el desempeño de su conexión de AWS Site-to-Site VPN. Debe recopilar datos de monitorización de todas las partes de su solución de AWS para que le resulte más sencillo depurar un error que se produce en distintas partes del código, en caso de que ocurra. No obstante, antes de comenzar a monitorizar su conexión de Site-to-Site VPN, debe crear un plan de monitorización que incluya respuestas a las siguientes preguntas:

- ¿Cuáles son los objetivos de la monitorización?
- ¿Qué recursos va a monitorizar?
- ¿Con qué frecuencia va a monitorizar estos recursos?
- ¿Qué herramientas de monitorización va a utilizar?
- ¿Quién se encargará de realizar las tareas de monitorización?
- ¿Quién debería recibir una notificación cuando surjan problemas?

El siguiente paso consiste en establecer un punto de referencia del desempeño de VPN normal en su entorno. Para ello se mide el desempeño en distintos momentos y bajo distintas condiciones de carga. A medida que monitorice su VPN, almacene los datos de monitorización históricos para que pueda compararlos con los datos de desempeño actual, identificar los patrones de desempeño normal y las anomalías en el desempeño, así como desarrollar métodos para la resolución de problemas.

Para establecer un punto de referencia, debe monitorizar los elementos siguientes:

- El estado de sus túneles de VPN
- Los datos que entran en el túnel
- Los datos que salen del túnel

Contenido

Herramientas de monitorización

AWS proporciona varias herramientas que puede utilizar para monitorizar una conexión de Site-to-Site VPN. Puede configurar algunas de estas herramientas para que monitoricen por usted, pero otras herramientas requieren intervención manual. Le recomendamos que automatice las tareas de monitorización en la medida de lo posible.

Herramientas de monitorización automatizadas

Puede utilizar las siguientes herramientas de monitorización automatizada para monitorizar una conexión de Site-to-Site VPN e informar cuando haya algún problema:

- Amazon CloudWatch Alarms (Alarmas de Amazon CloudWatch): observe una sola métrica durante el periodo que especifique y realice una o varias acciones según el valor de la métrica relativo a un

determinado umbral durante varios periodos de tiempo. La acción es una notificación enviada a un tema de Amazon SNS. Las alarmas de CloudWatch no invocan acciones simplemente por tener un estado determinado. Es necesario que el estado haya cambiado y se mantenga durante un número especificado de períodos. Para obtener más información, consulte Monitorización de túneles de VPN con Amazon CloudWatch (p. 30).

- AWS CloudTrail Log Monitoring (Monitorización de registros de AWS CloudTrail)–: compartir archivos de registro entre cuentas, monitorizar archivos de registro de CloudTrail en tiempo real mediante su envío a CloudWatch Logs, escribir aplicaciones de procesamiento de registros en Java y validar que sus archivos de registro no hayan cambiado después de que CloudTrail los entregue. Para obtener más información, consulte la sección sobre el registro de llamadas a la API mediante AWS CloudTrail en la Amazon EC2 API Reference y Trabajar con archivos de registro de CloudTrail en la AWS CloudTrail User Guide.

Herramientas de monitorización manual

Otra parte importante de la monitorización de una conexión de Site-to-Site VPN implica la monitorización manual de los elementos que no cubren las alarmas de CloudWatch. Los paneles de consola de Amazon VPC y de CloudWatch proporcionan una vista rápida del entorno de AWS.

- El panel de Amazon VPC muestra lo siguiente:
  - Estado de los servicios por región
  - Conexiones de Site-to-Site VPN
  - Estado del túnel de VPN (en el panel de navegación, elija Site-to-Site VPN Connections (Conexiones de Site-to-Site VPN), seleccione una conexión de Site-to-Site VPN y, a continuación, elija Tunnel Details (Detalles de túnel)).
- La página de inicio de CloudWatch muestra:
  - Alarmas y estado actual
  - Gráficos de alarmas y recursos
  - Estado de los servicios

  Además, puede utilizar CloudWatch para hacer lo siguiente:
  - Crear paneles personalizados para monitorizar los servicios que le interesan.
  - Realizar un gráfico con los datos de las métricas para resolver problemas y descubrir tendencias
  - Buscar y examinar todas sus métricas de recursos de AWS.
  - Crear y editar las alarmas de notificación de problemas

Monitorización de túneles de VPN con Amazon CloudWatch

Puede monitorizar los túneles de VPN mediante CloudWatch, que recopila y procesa los datos sin formato del servicio VPN en métricas legibles y casi en tiempo real. Estas estadísticas se registran durante un periodo de 15 meses, de forma que pueda obtener acceso a información de historial y obtener una mejor perspectiva acerca del desempeño de su aplicación web o servicio. Los datos de métricas de VPN se envían automáticamente a CloudWatch en cuanto estos están disponibles.

> **Important**
>
> Las métricas de CloudWatch no se pueden usar con conexiones AWS Classic VPN. Para obtener más información, consulte Categorías de AWS Site-to-Site VPN (p. 2).

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

Dimensiones y métricas de túneles de VPN

Las siguientes métricas están disponibles para los túneles de VPN.

Métrica	Descripción
`TunnelState`	El estado del túnel. Para las VPN estáticas, 0 indica DOWN y 1 indica UP. Para las VPN de BGP, 1 indica ESTABLISHED y 0 se utiliza para los demás estados. Unidades: booleano
`TunnelDataIn`	Los bytes recibidos a través del túnel de VPN. Cada punto de datos de la métrica representa el número de bytes recibidos después del punto de datos anterior. Use la estadística Sum para mostrar el número total de bytes recibidos durante el periodo. Esta métrica cuenta los datos después del descifrado. Unidades: bytes
`TunnelDataOut`	Los bytes enviados a través del túnel de VPN. 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

Para filtrar los datos de las métricas, use las siguientes dimensiones.

Dimensión	Descripción
`VpnId`	Filtra los datos de las métricas en función del ID de conexión de Site-to-Site VPN.
`TunnelIpAddress`	Filtra los datos de las métricas en función de la dirección IP del túnel de la gateway privada virtual.

Ver métricas de CloudWatch de túneles de VPN

Al crear una nueva conexión de Site-to-Site VPN, el servicio VPN envía las siguientes métricas acerca de sus túneles de VPN a CloudWatch en cuanto están disponibles. Puede ver las métricas de los túneles de VPN de la manera siguiente.

Para consultar las métricas desde la consola de CloudWatch

Las métricas se agrupan en primer lugar por el espacio de nombres de servicio y, a continuación, por las diversas combinaciones de dimensiones dentro de cada espacio de nombres.

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.

2. En el panel de navegación, seleccione Metrics.
3. En All metrics (Todas las métricas) elija el espacio de nombres de métricas VPN.
4. Seleccione la dimensión de métrica para ver las métricas (por ejemplo, para la conexión de Site-to-Site VPN).

Para ver métricas mediante la CLI de AWS

En el símbolo del sistema, ejecute el siguiente comando:

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

Creación de alarmas de CloudWatch para monitorizar túneles de VPN

Puede crear una alarma de CloudWatch 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 monitorice el estado de un túnel de VPN y envíe una notificación cuando el estado del túnel sea inactivo durante 3 periodos consecutivos de 5 minutos.

Para crear una alarma para el estado del túnel

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms, Create Alarm.
3. Elija VPN Tunnel Metrics.
4. Elija la dirección IP del túnel de VPN y la métrica TunnelState. Seleccione Siguiente.
5. Configure la alarma del modo que se indica y elija Create Alarm cuando haya terminado:
   - En Alarm Threshold, escriba el nombre y la descripción de la alarma. En Whenever (Siempre que), elija <= y escriba `0`. Escriba 3 para los periodos consecutivos.
   - En Actions, seleccione una notificación existente o elija New list para crear una.
   - En Alarm Preview (Vista previa de alarma), seleccione un periodo de 5 minutos y especifique una estadística de Maximum (Máximo).

Puede crear una alarma que monitorice el estado de la conexión de Site-to-Site VPN. Por ejemplo, la siguiente alarma envía una notificación cuando el estado de ambos túneles está INACTIVO durante un período consecutivo de 5 minutos.

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

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas), Create Alarm (Crear alarma).
3. Elija VPN Connection Metrics (Métricas de conexión de VPN).
4. Seleccione su conexión de Site-to-Site VPN y la métrica TunnelState. Elija Next (Siguiente).
5. Configure la alarma del modo que se indica y elija Create Alarm (Crear alarma) cuando haya terminado:
   - En Alarm Threshold, escriba el nombre y la descripción de la alarma. En Whenever (Siempre que), elija <= y escriba `0`. Escriba 1 para los periodos consecutivos.

- En Actions, seleccione una notificación existente o elija New list para crear una.
- En Alarm Preview (Vista previa de alarma), seleccione un periodo de 5 minutos y especifique una estadística de Maximum (Máximo).

  Como opción, si ha configurado su conexión de Site-to-Site VPN de modo que ambos túneles están activos, puede especificar una estadística Minimum (Mínimo) para enviar una notificación cuando haya al menos un túnel inactivo.

También puede crear alarmas que monitoricen la cantidad de tráfico que entra o sale del túnel de VPN. Por ejemplo, la siguiente alarma monitoriza la cantidad de tráfico que entra en el túnel de VPN desde su red, y envía una notificación cuando el número de bytes alcanza un umbral de 5 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red entrante

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas), Create Alarm (Crear alarma).
3. Elija VPN Tunnel Metrics.
4. Seleccione la dirección IP del túnel de VPN y la métrica TunnelDataIn. Elija Next (Siguiente).
5. Configure la alarma del modo que se indica y elija Create Alarm (Crear alarma) cuando haya terminado:

   - En Alarm Threshold, escriba el nombre y la descripción de la alarma. En Whenever, elija **>=** y escriba `5000000`. Escriba 1 para los periodos consecutivos.
   - En Actions, seleccione una notificación existente o elija New list para crear una.
   - En Alarm Preview, seleccione un periodo de 15 minutos y especifique una estadística de Sum.

La siguiente alarma monitoriza la cantidad de tráfico que sale del túnel de VPN a su red, y envía una notificación cuando el número de bytes sea inferior a 1 000 000 durante un periodo de 15 minutos.

Para crear una alarma para el tráfico de red saliente

1. Abra la consola de CloudWatch en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Alarms (Alarmas), Create Alarm (Crear alarma).
3. Elija VPN Tunnel Metrics.
4. Seleccione la dirección IP del túnel de VPN y la métrica TunnelDataOut. Elija Next (Siguiente).
5. Configure la alarma del modo que se indica y elija Create Alarm (Crear alarma) cuando haya terminado:

   - En Alarm Threshold, escriba el nombre y la descripción de la alarma. En Whenever (Siempre que), elija **<=** y escriba `1000000`. Escriba 1 para los periodos consecutivos.
   - En Actions, seleccione una notificación existente o elija New list para crear una.
   - En Alarm Preview, seleccione un periodo de 15 minutos y especifique una estadística de Sum.

Para obtener más ejemplos de creación de alarmas, consulte Creación de alarmas de Amazon CloudWatch en la Guía del usuario de Amazon CloudWatch.

Historial de versiones

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

Cambio	Descripción	Fecha
Puede modificar la gateway de destino de la conexión de AWS Site-to-Site VPN	Puede modificar la gateway de destino de la conexión de AWS Site-to-Site VPN. Para obtener más información, consulte Modificación de una gateway de destino de la conexión de Site-to-Site VPN (p. 22).	18 de diciembre de 2018
Versión inicial	En esta versión, se separa el contenido de AWS Site-to-Site VPN (anteriormente conocido como AWS Managed VPN) del de la Guía del usuario de Amazon VPC.	18 de diciembre de 2018