AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

¿Qué es AWS Transit Gateway para Amazon VPC?

AWS Transit Gateway es un centro de tránsito de red que se utiliza para interconectar nubes privadas virtuales (VPC) y redes locales. A medida que su infraestructura de nube se expande a nivel mundial, la interconexión entre regiones conecta las pasarelas de tránsito entre sí mediante la infraestructura global. AWS Todo el tráfico de red entre centros de datos de AWS se cifra automáticamente en la capa física.

Para obtener más información, consulte el sitio web de AWS Transit Gateway.

Conceptos de las gateways de tránsito

A continuación, se muestran conceptos clave para gateways de tránsito:

- Conexiones: puede asociar lo siguiente:
  - Una o varias VPC
  - Un dispositivo SD-WAN/third-party de red Connect
  - Una AWS Direct Connect puerta de enlace
  - Una conexión de pares con otra gateway de tránsito
  - Una conexión de VPN a una gateway de tránsito
  - De un concentrador de VPN a una pasarela de tránsito
  - Un punto final de Client VPN a una puerta de enlace de tránsito
  - Una conexión de función de red. Para obtener más información, consulte the section called “Vinculaciones de funciones de red”.
- Unidad máxima de transferencia (MTU) de gateway de tránsito: la unidad máxima de transferencia (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede pasar a través de la conexión. Cuanto mayor sea la MTU de una conexión, mayor cantidad de datos se podrán transferir en un solo paquete. Una puerta de enlace de tránsito admite una MTU de 8500 bytes para el tráfico entre las VPC, Transit Direct Connect Gateway Connect y los archivos adjuntos de emparejamiento (archivos adjuntos de emparejamiento intrarregionales, interregionales y de WAN en la nube). El tráfico a través de conexiones de VPN puede tener una MTU de 1500 bytes.
- Control de cifrado: se puede configurar una puerta de enlace de tránsito para que sea compatible con el control de cifrado, que aplica el cifrado en tránsito para todo el tráfico de las VPC

conectadas a la puerta de enlace de tránsito. Cuando el control de cifrado está habilitado, la puerta de enlace de tránsito se puede conectar a las VPC con el control de cifrado aplicado. Esta función garantiza que todo el tráfico que fluye a través de la pasarela de tránsito esté cifrado, lo que proporciona una mayor seguridad para las comunicaciones de la red.

- Tabla de enrutamiento de gateway de tránsito: una gateway de tránsito tiene una tabla de enrutamiento predeterminada y, opcionalmente, puede tener tablas de enrutamiento adicionales. Una tabla de ruteo incluye rutas dinámicas y estáticas que deciden el siguiente salto en función de la dirección IP de destino del paquete. El objetivo de estas rutas podría ser cualquier conexión de gateway de tránsito. De forma predeterminada, la puerta de enlaces de tránsito está asociada con la tabla de enrutamiento de la gateway de tránsito predeterminada.
- Asociaciones: cada conexión se asocia con una sola tabla de enrutamiento. Cada tabla de ruteo puede asociarse con un número de cero a varias vinculaciones.
- Propagación de rutas: una conexión de VPC o de VPN o gateway de Direct Connect puede propagar rutas a una tabla de enrutamiento de una gateway de tránsito de forma dinámica. Con una conexión de Connect, las rutas se propagan a una tabla de enrutamiento de gateway de tránsito de forma predeterminada. Con una VPC, debe crear rutas estáticas para enviar el tráfico a la gateway de tránsito. Con una conexión de VPN, las rutas se propagan desde la gateway de tránsito hasta el enrutador local con el protocolo de gateway fronteriza (BGP). Con una puerta de enlace de Direct Connect, los prefijos permitidos se originan en el enrutador en las instalaciones mediante el BGP. Con una vinculación de interconexión, debe crear una ruta estática en la tabla de enrutamiento de la gateway de tránsito hasta el punto de la vinculación de interconexión.

Introducción a las gateways de tránsito

Utilice los siguientes recursos para ayudarle a crear y utilizar una gateway de tránsito.

- Cómo funcionan las puertas de enlace de tránsito
- Introducción a las puertas de enlace de tránsito
- Prácticas recomendadas de diseño

Utilizar gateways de tránsito

Puede crear, acceder y administrar las gateways de tránsito con cualquiera de las siguientes interfaces:

- Consola de administración de AWS — proporciona una interfaz web que se puede utilizar para obtener acceso a las gateways de tránsito.
- AWS Interfaz de línea de comandos (AWS CLI): proporciona comandos para un amplio conjunto de AWS servicios, incluida Amazon VPC, y es compatible con Windows, macOS y Linux. Para obtener más información, consulte AWS Command Line Interface.
- AWS SDK: proporciona operaciones de API específicas del idioma y se ocupa de muchos de los detalles de la conexión, como el cálculo de las firmas, la gestión de los reintentos de solicitudes y la gestión de los errores. Para obtener más información, consulte AWS SDK.
- API de consulta: proporciona acciones de API de nivel bajo a las que se llama mediante solicitudes HTTPS. El uso de la API de consulta es la forma más directa de acceder a Amazon VPC, pero requiere que la aplicación controle niveles de detalle de bajo nivel, como la generación de hash para firmar la solicitud y el control de errores. Para obtener más información, consulte la referencia de las API de Amazon EC2.

Precios

Se le cobrará por hora por cada conexión en una gateway de tránsito y se le cobrará la cantidad de tráfico procesado en la gateway de tránsito. De forma predeterminada, los cargos por procesamiento de datos se asignan a la cuenta propietaria del archivo adjunto de origen. Puede utilizar una asignación de costes flexible para personalizar la forma en que se asignan estos cargos en función de las necesidades de su organización. Para obtener más información, consulte los precios de AWS Transit Gateway yAsignación flexible de costes.

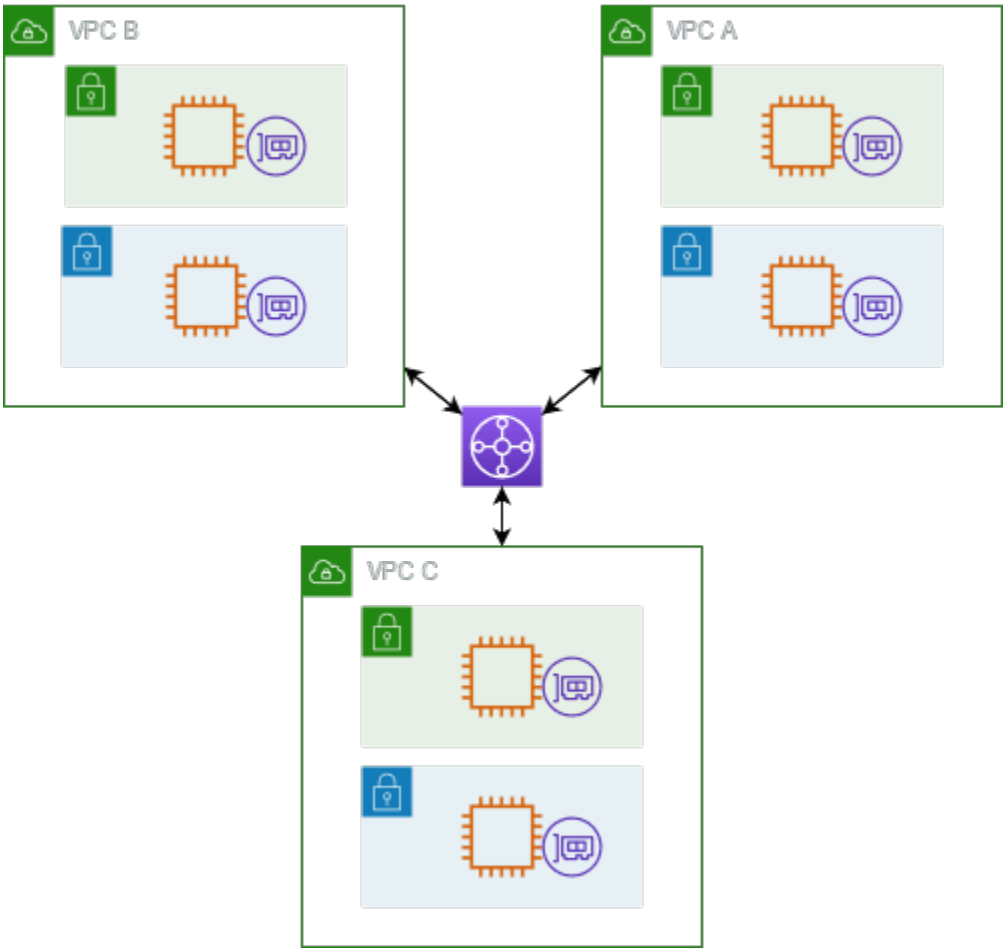
Cómo funciona AWS Transit Gateway

En AWS Transit Gateway, una puerta de enlace de tránsito actúa como un enrutador virtual regional para el tráfico que fluye entre sus nubes privadas virtuales (VPC) y las redes locales. Una puerta de enlace de tránsito se escala de manera elástica en función del volumen de tráfico de red. El enrutamiento a través de una puerta de enlace de tránsito funciona en la capa 3, donde los paquetes se envían a una conexión específica del siguiente salto en función de las direcciones IP de destino.

Temas

Ejemplo de un diagrama de arquitectura

El diagrama siguiente muestra una puerta de enlace de tránsito con tres VPC adjuntas. La tabla de enrutamiento de cada una de estas VPC incluye la ruta local y las rutas que envían tráfico destinado a las otras dos VPC a la puerta de enlace de tránsito.



A continuación, se muestra un ejemplo de una tabla de enrutamiento de puerta de enlace de tránsito predeterminada para los adjuntos que aparecen en el diagrama anterior. Los bloques de CIDR de cada VPC se propagan a la tabla de enrutamiento. Por lo tanto, cada adjunto puede dirigir paquetes a los otros dos adjuntos.

Destino	Objetivo	Tipo de ruta
VPC A CIDR	*Attachment for VPC A*	propagada
VPC B CIDR	*Attachment for VPC B*	propagada
VPC C CIDR	*Attachment for VPC C*	propagada

Vinculaciones de recursos

Una conexión de puerta de enlace de tránsito es origen y destino de paquetes. Puede asociar los siguientes recursos a la puerta de enlace de tránsito:

- Una o más VPC. AWS Transit Gateway implementa una interfaz de red elástica en las subredes de VPC, que luego utiliza la puerta de enlace de tránsito para enrutar el tráfico hacia y desde las subredes elegidas. Debe tener al menos una subred para cada zona de disponibilidad, lo que permite que el tráfico llegue a los recursos de todas las subredes de dicha zona. Durante la creación de una conexión, los recursos de una zona de disponibilidad determinada solo pueden llegar a una puerta de enlace de tránsito si una subred está habilitada dentro de la misma zona. Si una tabla de enrutamiento de subred incluye una ruta a la puerta de enlace de tránsito, el tráfico solo se reenvía a la puerta de enlace de tránsito cuando la gateway de tránsito tenga una conexión en una subred en la misma zona de disponibilidad.
- Una o varias conexiones de VPN
- Uno o más concentradores de VPN
- Una o más AWS Direct Connect puertas de enlace
- Una o varias vinculaciones de Transit Gateway Connect
- Una o más interconexiones de puerta de enlace de tránsito

Enrutamiento multiruta de igual costo

AWS Transit Gateway admite el enrutamiento de rutas múltiples de igual costo (ECMP) para la mayoría de los accesorios. Para una conexión de VPN, puede habilitar o deshabilitar la compatibilidad con ECMP mediante la consola al crear o modificar una puerta de enlace de tránsito. Para todos los demás tipos de conexiones, se aplican las siguientes restricciones de ECMP:

- VPC: la VPC no admite ECMP, ya que los bloques CIDR no se pueden superponer. Por ejemplo, no puede adjuntar una VPC con un CIDR 10.1.0. 0/16 con una segunda VPC que utilice el mismo CIDR para una puerta de enlace de tránsito y, a continuación, configure el enrutamiento para equilibrar la carga del tráfico entre ellas.
- VPN: cuando la opción de compatibilidad con ECMP de VPN está deshabilitada, una puerta de enlace de tránsito utiliza métricas internas para determinar la ruta preferida en caso de que haya prefijos iguales en varias rutas. Para obtener más información sobre cómo habilitar o deshabilitar el ECMP para una conexión de VPN, consulte the section called “Puertas de enlace de tránsito”.

- AWS Transit Gateway Connect: los accesorios AWS Transit Gateway Connect admiten automáticamente el ECMP.
- AWS Direct Connect Puerta de enlace: los adjuntos de la AWS Direct Connect puerta de enlace admiten automáticamente el ECMP en varios archivos adjuntos de Direct Connect Gateway cuando el prefijo de red, la longitud del prefijo y AS_PATH son exactamente iguales.
- Interconexión de puertas de enlace de tránsito: la interconexión de puertas de enlace de tránsito no admite ECMP, ya que no admite el enrutamiento dinámico ni puede configurar la misma ruta estática para dos destinos diferentes.
- Concentrador VPN: el concentrador VPN no es compatible con ECMP.

> **Note**
>
> - No se admite BGP Multipath AS-Path Relax, por lo que no puede usar el ECMP con diferentes números de sistema autónomo (ASN).
> - El ECMP no se admite entre diferentes tipos de conexiones. Por ejemplo, no puede habilitar el ECMP entre una VPN y una conexión de VPC. En su lugar, las rutas de puerta de enlace de tránsito se evalúan y el tráfico se enruta de acuerdo con la ruta evaluada. Para obtener más información, consulte the section called “Orden de evaluación de rutas”.
> - Una única puerta de enlace de Direct Connect admite ECMP en varias interfaces virtuales de tránsito. Por lo tanto, le recomendamos que configure y utilice solo una puerta de enlace de Direct Connect y que no configure ni utilice varias puertas de enlace para aprovechar el ECMP. Para obtener más información sobre las puertas de enlace Direct Connect y las interfaces virtuales públicas, consulte ¿Cómo Active/Active configuro una conexión de Active/Passive Direct Connect AWS desde una interfaz virtual pública? .

Zonas de disponibilidad

Al asociar una VPC a una puerta de enlace de tránsito, debe habilitar una o varias zonas de disponibilidad que la puerta de enlace de tránsito utilizará para enrutar el tráfico a los recursos de las subredes de VPC. Para habilitar cada una de las zonas de disponibilidad, solo debe especificar una subred. La puerta de enlace de tránsito ubica una interfaz de red en esa subred con una dirección IP de la subred. Una vez que haya habilitado una zona de disponibilidad mediante la especificación de una subred, el tráfico se puede dirigir a todas las subredes de dicha zona, no solo a la subred

especificada. Sin embargo, solo los recursos que residen en zonas de disponibilidad donde hay una conexión de puerta de enlace de tránsito pueden llegar a la puerta de enlace de tránsito.

Si el tráfico proviene de una zona de disponibilidad en la que el adjunto de destino no está presente, AWS Transit Gateway enrutará internamente ese tráfico a una zona de disponibilidad aleatoria en la que esté presente el adjunto. No se aplica ningún cargo adicional a la puerta de enlace de tránsito para este tipo de tráfico entre zonas de disponibilidad.

Se recomienda habilitar varias zonas de disponibilidad para garantizar la disponibilidad.

Uso de la compatibilidad del modo dispositivo

Si piensa configurar un dispositivo de red con estado en la VPC, puede habilitar la compatibilidad en modo dispositivo para la conexión de VPC en la que se encuentra la aplicación. Esto garantiza que la puerta de enlace de tránsito utilice la misma zona de disponibilidad para esa conexión de VPC durante la vida útil de un flujo de tráfico entre el origen y el destino. También permite que la puerta de enlace de tránsito envíe tráfico a cualquier zona de disponibilidad de la VPC, siempre y cuando exista una asociación de subred en esa zona. Para obtener más información, consulte Ejemplo: Dispositivo en una VPC de servicios compartidos.

Enrutamiento

La puerta de enlace de tránsito enruta paquetes de IPv4 e IPv6 entre conexiones mediante tablas de enrutamiento de puerta de enlace de tránsito. Puede configurar dichas tablas para propagar rutas desde las tablas de enrutamiento para las VPC, las conexiones VPN y las puertas de enlace de Direct Connect. También puede agregar rutas estáticas a las tablas de enrutamiento de la puerta de enlace de tránsito. Cuando un paquete proviene de una vinculación, se enruta a otra distinta mediante la ruta que coincide con la dirección IP de destino.

Solo las rutas estáticas son compatibles para las vinculaciones de interconexión de puerta de enlace de tránsito.

Temas de enrutamiento

- Tablas de enrutamiento
- Asociación de tabla de enrutamiento
- Propagación de rutas
- Rutas para las vinculaciones de interconexiones

- Orden de evaluación de rutas

Tablas de enrutamiento

La puerta de enlace de tránsito viene automáticamente con una tabla de enrutamiento predeterminada. Esta es la tabla de enrutamiento de asociación y de propagación predeterminada. Si deshabilita tanto la propagación de rutas como la asociación de tablas de rutas, AWS no crea una tabla de rutas predeterminada para la pasarela de tránsito. Sin embargo, si la propagación de rutas o la asociación de tablas de rutas están AWS habilitadas, crea una tabla de rutas predeterminada.

Puede crear tablas de enrutamiento adicionales para la puerta de enlace de tránsito. Esto le permite aislar los subconjuntos de las vinculaciones. Cada vinculación se puede asociar con una tabla de enrutamiento. Una vinculación puede propagar sus rutas a una o más tablas de enrutamiento.

Puede crear una ruta de agujero negro en la tabla de enrutamiento de puerta de enlace de tránsito que reduce el tráfico que coincide con la ruta.

Al vincular una VPC a una puerta de enlace de tránsito, debe agregar una ruta a la tabla de enrutamiento de subred para que el tráfico se enrute a través de la puerta de enlace de tránsito. Para obtener más información, consulte Enrutamiento para una Transit Gateway en la Guía del usuario de Amazon VPC.

Asociación de tabla de enrutamiento

Puede asociar una puerta de enlaces de tránsito con una sola tabla de enrutamiento. Cada tabla de este tipo se puede asociar a un número variable de cero a varias vinculaciones y puede reenviar los paquetes a otras vinculaciones.

Propagación de rutas

Cada conexión incluye rutas que se pueden instalar en una o más tablas de enrutamiento de puerta de enlace de tránsito. Al propagarse una conexión a una tabla de enrutamiento de puerta de enlace de tránsito, estas rutas se instalan en la tabla. No es posible filtrar rutas anunciadas.

Para una vinculación de VPC, los bloques de CIDR de la VPC se propagan a la tabla de enrutamiento de la puerta de enlace de tránsito.

Cuando se utiliza el enrutamiento dinámico con un adjunto de VPN, un adjunto de VPN Concentrator o un adjunto de puerta de enlace Direct Connect, puede propagar las rutas aprendidas desde el router local a través de BGP a cualquiera de las tablas de rutas de la puerta de enlace de tránsito.

Cuando el enrutamiento dinámico se utiliza con un adjunto de VPN o un adjunto de concentrador de VPN, las rutas de la tabla de rutas asociadas al adjunto de VPN o al adjunto de concentrador de VPN se anuncian en la pasarela del cliente mediante BGP.

En el caso de un adjunto de Connect, las rutas de la tabla de enrutamiento asociada al adjunto de Connect se anuncian en los dispositivos virtuales de terceros, como SD-WAN los dispositivos, que se ejecutan en una VPC a través de BGP.

En el caso de un adjunto a una pasarela Direct Connect, las interacciones con los prefijos permitidos controlan las rutas desde las que se anuncian en la red del cliente. AWS

Cuando una ruta estática y una ruta propagada tienen el mismo destino, la ruta estática tiene la prioridad más alta, por lo que la ruta propagada no se incluye en la tabla de enrutamiento. Si elimina la ruta estática, la ruta propagada superpuesta se incluirá en la tabla de enrutamiento.

Rutas para las vinculaciones de interconexiones

Puede unir dos puertas de enlace de tránsito y dirigir el tráfico entre ellas. Para ello, se debe crear una conexión de interconexión en la puerta de enlace de tránsito y especificar la puerta de enlace de tránsito de interconexión con la que crear la interconexión. A continuación, se crea una ruta estática en la tabla de enrutamiento de la gateway de tránsito para enrutar el tráfico a la conexión de la gateway de tránsito. El tráfico que se enruta a la gateway de tránsito de interconexión se puede enrutar a las conexiones de VPN y VPC para la puerta de enlace de tránsito de interconexión.

Para obtener más información, consulte Ejemplo: gateways de tránsito interconectadas.

Orden de evaluación de rutas

Las rutas de puerta de enlace de tránsito se evalúan en el siguiente orden:

- La ruta más específica para la dirección de destino.
- En el caso de las rutas con el mismo CIDR, pero con tipos de conexiones diferentes, la prioridad de las rutas es la siguiente:
  - Rutas estáticas (por ejemplo, rutas estáticas de Site-to-Site VPN)
  - rutas de lista de prefijos de referencia
  - VPC-propagated rutas
  - Rutas propagadas por la puerta de enlace de Direct Connect
  - Connect-propagated Rutas de Transit Gateway

- Site-to-Site VPN a través de Connect-propagated rutas directas privadas
- Site-to-Site VPN-propagated rutas
- Site-to-Site VPN-Concentrator rutas propagadas
- Rutas propagadas por Client VPN
- Rutas propagadas por la interconexión de Transit Gateway (Cloud WAN)

Algunas conexiones son compatibles con el anuncio de rutas a través de BGP. En el caso de las rutas con el mismo CIDR y que son del mismo tipo de conexión, la prioridad de las rutas está controlada por los atributos de BGP:

- Ruta AS más corta
- Valor MED más bajo
- Se prefieren las rutas eBGP sobre las iBGP, siempre que la conexión sea compatible.

> **Important**
>
> - AWS no se puede garantizar un orden de priorización de rutas coherente para las rutas BGP con el mismo CIDR, tipo de adjunto y atributos de BGP que los enumerados anteriormente.
> - Para las rutas anunciadas a una puerta de enlace de tránsito sin MED, AWS Transit Gateway asignará los siguientes valores predeterminados:
>   - 0 para las rutas entrantes anunciadas en las vinculaciones de Direct Connect.
>   - 100 para las rutas entrantes anunciadas en la VPN y las vinculaciones de Connect.

AWS Transit Gateway solo muestra una ruta preferida. Una ruta de respaldo solo aparecerá en la tabla de rutas de la puerta de enlace de tránsito si la ruta anteriormente activa ya no se anuncia, por ejemplo, si anuncia las mismas rutas a través de la puerta de enlace Direct Connect y de la Site-to-Site VPN. AWS Transit Gateway solo mostrará las rutas recibidas desde la ruta de puerta de enlace Direct Connect, que es la ruta preferida. La Site-to-Site VPN, que es la ruta de respaldo, solo se mostrará cuando la puerta de enlace Direct Connect deje de estar anunciada.

Diferencias entre las tablas de enrutamiento de la VPC y de la puerta de enlace de tránsito

La evaluación de la tabla de enrutamiento difiere entre si se utiliza una tabla de enrutamiento de VPC o una tabla de enrutamiento de la puerta de enlace de tránsito.

En el ejemplo a continuación se muestra una tabla de enrutamiento de VPC. La ruta local de VPC tiene la prioridad más alta, seguida por las rutas más específicas. Cuando una ruta estática y una ruta propagada tienen el mismo destino, la ruta estadística tiene una prioridad más elevada.

Destino	Objetivo	Priority (Prioridad)
10.0.0. 0/16	local	1
192.168.0. 0/16	pcx-12345	2
172,31,0. 0/16	vgw-12345 (estática) o tgw-12345 (estática)	2
172,31,0. 0/16	vgw-12345 (propagada)	3
0.0.0. 0/0	igw-12345	4

En el ejemplo a continuación se muestra una tabla de enrutamiento de la puerta de enlace de tránsito. Si prefiere utilizar la conexión de la puerta de enlace de Direct Connect en la vinculación de la VPN, utilice una conexión de VPN del BGP y propague las rutas en la tabla de enrutamiento de puerta de enlace de tránsito.

Destino	Vinculación (objetivo)	Tipo de recurso	Tipo de ruta	Priority (Prioridad)
10.0.0. 0/16	tgw-attach-123 | vpc-1234	VPC	Estático o propagado	1
192.168.0. 0/16	tgw-attach-789 | vpn-5678	VPN	Estático	2

Destino	Vinculación (objetivo)	Tipo de recurso	Tipo de ruta	Priority (Priorida d)
172,31,0. 0/16	tgw-attach-456 | dxgw_id	Direct Connect gateway	Propagado	3
172,31,0. 0/16	tgw-attach-789 | tgw-connect-peer-123	Conexión	Propagado	4
172,31,0. 0/16	tgw-attach-789 | vpn-5678	VPN	Propagado	5

Vinculaciones de funciones de red

Un adjunto de función de red es un recurso que conecta una función de seguridad de red (por ejemplo, un AWS Network Firewall adjunto) directamente a su pasarela de transporte. Elimina la necesidad de crear y administrar manualmente las VPC de inspección.

Con una conexión de función de red:

- AWS crea y administra automáticamente la infraestructura subyacente
- El tráfico se puede inspeccionar a medida que fluye a través de su puerta de enlace de transporte
- Las políticas de seguridad se aplican de forma uniforme en toda la red

- Puede dirigir el tráfico a través del firewall mediante reglas de enrutamiento sencillas
- La vinculación funciona en varias zonas de disponibilidad para obtener una alta disponibilidad

Esta integración simplifica la seguridad de la red al permitirle conectar los firewalls directamente a su puerta de enlace de tránsito en lugar de crear configuraciones de enrutamiento complejas y administrar puntos de conexión separados a través de VPC independientes.

AWS Network Firewall integración

AWS Network Firewall la integración le permite conectar un firewall en forma de un grupo de puntos finales del Gateway Load Balancer, uno por zona de disponibilidad, en una VPC con búfer

gestionada por el servicio. Se crea una vinculación de firewall de red con el modo dispositivo activado de manera automática. Esto elimina la necesidad de administrar de manera explícita las VPC de inspección.

Con la integración del firewall de red, ya no necesita crear y administrar VPC de inspección para sus implementaciones de firewall de red. En lugar de seleccionar una VPC y subredes al crear el firewall, selecciona directamente la puerta de enlace de tránsito y AWS aprovisiona y administra automáticamente todos los recursos necesarios entre bastidores. Verá una nueva conexión de función de red de la puerta de enlace de tránsito en lugar de un punto de conexión de firewall individual.

En escenarios de varias cuentas, la Transit Gateway puede ser RAM-shared desde el propietario de Transit Gateway hasta la cuenta de propietario de Network Firewall, lo que permite que cualquiera de las cuentas administre el adjunto del firewall. Una vez que el firewall y la vinculación estén listos, solo tiene que modificar las tablas de enrutamiento de la puerta de enlace de tránsito para enviar el tráfico a la vinculación para su inspección.

> **Note**
>
> - La puerta de enlace de tránsito es compatible únicamente con el enrutamiento estático en las vinculaciones del firewall de red.
> - Third-party No se admiten firewalls.

Para obtener más información sobre los firewalls y las vinculaciones, consulte Vinculaciones de función de red de puerta de enlace de tránsito.

Ejemplos de escenarios de la puerta de enlace de tránsito

A continuación, se muestran casos de uso comunes para gateways de tránsito. Sus gateways de tránsito no se limitan a estos casos de uso.

Ejemplo: enrutador centralizado

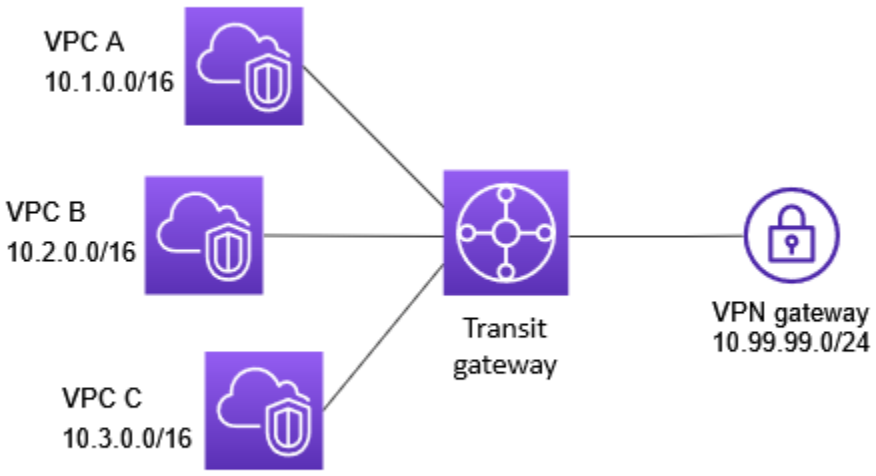
Puede configurar su puerta de enlace de tránsito como un enrutador centralizado que conecte todas sus VPC y conexiones Site-to-Site VPN. AWS Direct Connect En este escenario, todas las vinculaciones se asocian a la tabla de enrutamiento predeterminada de la puerta de enlace de

tránsito y se propagan a la tabla de enrutamiento predeterminada de la gateway de tránsito. Por lo tanto, todas las conexiones pueden enrutar paquetes entre sí y la puerta de enlace de tránsito actúa como un enrutador de IP de capa 3 simple.

Contenido

Descripción general de

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. En este escenario, hay tres adjuntos de VPC y un adjunto de Site-to-Site VPN a la puerta de enlace de tránsito. Los paquetes de las subredes en VPC A, VPC B y VPC C que están destinados a una subred en otra VPC o para la conexión de VPN se enrutan primero a través de la puerta de enlace de tránsito.



Recursos

Cree los siguientes recursos para este escenario:

- Tres VPC Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.

- Una puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
- Tres conexiones de VPC en la gateway de tránsito. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
- Un adjunto de Site-to-Site VPN en la puerta de enlace de tránsito. Los bloques de CIDR de cada VPC se propagan a la tabla de enrutamiento de la puerta de enlace de tránsito. Cuando la conexión VPN está activa, se establece la sesión de BGP y el CIDR de la Site-to-Site VPN se propaga a la tabla de rutas de la puerta de enlace de tránsito y los CIDR de la VPC se agregan a la tabla BGP de la puerta de enlace del cliente. Para obtener más información, consulte the section called “Crear una vinculación de la puerta de enlace de tránsito a una VPN”.

  Asegúrese de revisar los requisitos para su dispositivo de puerta de enlace de cliente en la Guía del usuario de AWS Site-to-Site VPN .

Enrutamiento

Cada VPC cuenta con una tabla de enrutamiento y hay una tabla de enrutamiento para la puerta de enlace de tránsito.

Tablas de enrutamiento de la VPC

Cada VPC tiene una tabla de enrutamiento con 2 entradas. La primera fila es la entrada predeterminada para el direccionamiento IPv4 local de la VPC. Esta entrada permite a las instancias de esta VPC comunicarse entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la gateway de tránsito. La siguiente table muestra las rutas de VPC A.

Destino	Target
10.1.0. 0/16	local
0.0.0. 0/0	tgw-id

Tabla de enrutamiento de la puerta de enlace de tránsito

A continuación, se muestra un ejemplo de una tabla de enrutamiento predeterminada para las vinculaciones que aparecen en el diagrama anterior, con la propagación de rutas habilitada.

Destino	Objetivo	Tipo de ruta
10.1.0. 0/16	*Attachment for VPC A*	propagada
10.2.0. 0/16	*Attachment for VPC B*	propagada
10.3.0. 0/16	*Attachment for VPC C*	propagada
10.99,99. 0/24	*Attachment for VPN connection*	propagada

Tabla del BGP de la puerta de enlace de cliente

La tabla del número de sistema autónomo de la puerta de enlace de cliente contiene los siguientes CIDR de VPC.

- 10.1.0. 0/16
- 10.2.0. 0/16
- 10.3.0. 0/16

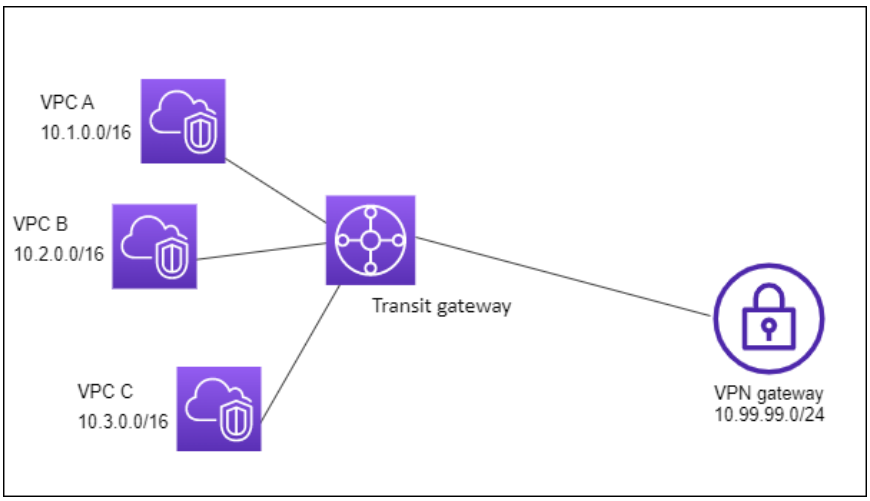
Ejemplo: VPC aisladas

Puede configurar la gateway de tránsito como varios enrutadores aislados. Es similar a utilizar varias gateways de tránsito, pero ofrece mayor flexibilidad en aquellos casos en los que es posible que las rutas y las conexiones cambien. En este escenario, cada router aislado tiene una sola tabla de ruteo. Todas las vinculaciones asociadas a un router aislado se propagan y se asocian en su tabla de ruteo. Las vinculaciones asociadas a un router aislado pueden dirigir paquetes entre sí, pero no pueden dirigir paquetes ni recibirlos de vinculaciones de otro router aislado.

Contenido

Descripción general de

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. Los paquetes de VPC A, VPC B y VPC C se enrutan a la gateway de tránsito. Los paquetes de las subredes de la VPC A, la VPC B y la VPC C que tienen Internet como destino se enrutan primero a través de la puerta de enlace de tránsito y, a continuación, a la conexión VPN (si Site-to-Site el destino está dentro de esa red). Los paquetes de una VPC que tienen un destino de una subred en otra VPC, por ejemplo, de 10.1.0.0 a 10.2.0.0, se enrutan a través de una gateway de tránsito, donde se bloquean porque no existe una ruta para ellos en la tabla de enrutamiento de la gateway de tránsito.



Recursos

Cree los siguientes recursos para este escenario:

- Tres VPC Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
- Una puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
- Tres conexiones en la gateway de tránsito para las tres VPC. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
- Un adjunto de Site-to-Site VPN en la puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una vinculación de la puerta de enlace de tránsito a una VPN”. Asegúrese de revisar los requisitos para su dispositivo de puerta de enlace de cliente en la Guía del usuario de AWS Site-to-Site VPN .

Cuando la conexión de VPN se activa, se establece la sesión de BGP y el CIDR de VPN se propaga a la tabla de enrutamiento de puerta de enlace de tránsito y los CIDR de la VPC se agregan a la tabla de BGP de la puerta de enlace de cliente.

Enrutamiento

Cada VPC tiene una tabla de enrutamiento y la gateway de tránsito tiene dos tablas de enrutamiento: una para las VPC y otra para la conexión de VPN.

Tablas de enrutamiento de VPC A, VPC B y VPC C

Cada VPC tiene una tabla de ruteo con 2 entradas. La primera fila es la entrada predeterminada para el direccionamiento IPv4 local de la VPC. Esta entrada habilita a las instancias de esta VPC a comunicarse entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la gateway de tránsito. La siguiente table muestra las rutas de VPC A.

Destino	Target
10.1.0. 0/16	local
0.0.0. 0/0	tgw-id

Tablas de enrutamiento de la gateway de tránsito

Este escenario utiliza una tabla de enrutamiento para las VPC y una tabla de enrutamiento para la conexión de VPN.

Las vinculaciones de la VPC están asociadas con la siguiente tabla de enrutamiento, que tiene una ruta propagada para la vinculación de la VPN.

Destino	Objetivo	Tipo de ruta
10.99,99. 0/24	*Attachment for VPN connection*	propagada

La vinculación de la VPN se asocia a la siguiente tabla de enrutamiento, que tiene rutas propagadas para cada una de las vinculaciones de la VPC.

Destino	Objetivo	Tipo de ruta
10.1.0. 0/16	*Attachment for VPC A*	propagada
10.2.0. 0/16	*Attachment for VPC B*	propagada
10.3.0. 0/16	*Attachment for VPC C*	propagada

Para obtener más información sobre la propagación de rutas en una tabla de enrutamiento de gateway de tránsito, consulte Habilitar la propagación de rutas a una tabla de rutas de Transit Gateway en AWS Transit Gateway.

Tabla del BGP de la gateway de cliente

La tabla del número de sistema autónomo de la puerta de enlace de cliente contiene los siguientes CIDR de VPC.

- 10.1.0. 0/16
- 10.2.0. 0/16
- 10.3.0. 0/16

Ejemplo: VPC aisladas con servicios compartidos

Una puerta de enlace de tránsito se puede configurar como varios enrutadores aislados que utilizan un servicio compartido. Es similar a utilizar varias puerta de enlaces de tránsito, pero ofrece mayor flexibilidad en aquellos casos en los que es posible que las rutas y las conexiones cambien. En este escenario, cada router aislado tiene una sola tabla de ruteo. Todas las vinculaciones asociadas a un router aislado se propagan y se asocian en su tabla de ruteo. Las vinculaciones asociadas a un router aislado pueden dirigir paquetes entre sí, pero no pueden dirigir paquetes ni recibirlos de vinculaciones de otro router aislado. Las vinculaciones pueden dirigir paquetes o recibirlos desde servicios compartidos. Puede utilizar este escenario cuando tenga grupos que tenga que estar aislados, pero utilizar un servicio compartido; por ejemplo, un sistema de producción.

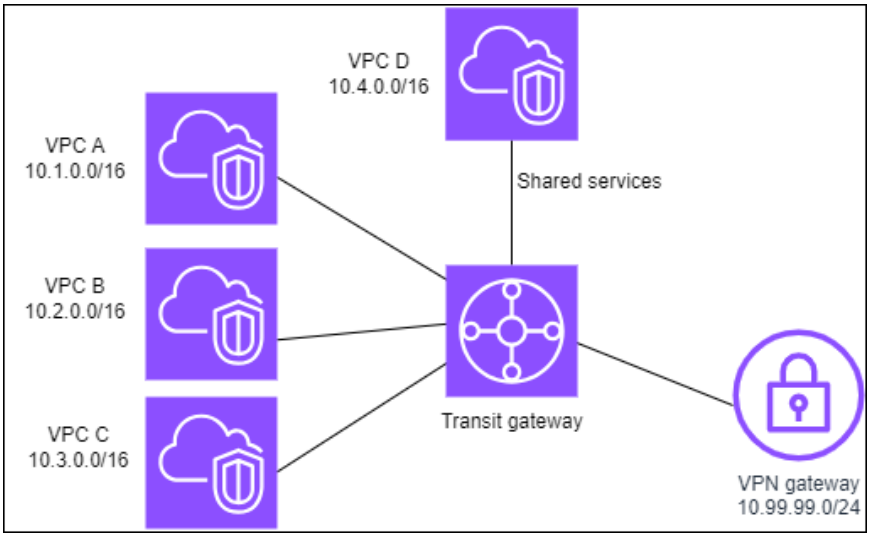
Contenido

- Descripción general de

- Recursos
- Enrutamiento

Descripción general de

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. Los paquetes de las subredes de la VPC A, la VPC B y la VPC C que tienen Internet como destino, primero se enrutan a través de la puerta de enlace de tránsito y, a continuación, a la puerta de enlace del cliente para la VPN. Site-to-Site Los paquetes de subredes en VPC A, VPC B o VPC C que tienen un destino de una subred en VPC A, VPC B o VPC C se enrutan a través de la puerta de enlace de tránsito, donde están bloqueados porque no hay ruta para ellos en la tabla de enrutamiento de la puerta de enlace de tránsito. Paquetes de VPC A, VPC B y VPC C que tengan VPC D como ruta de destino a través de la puerta de enlace de tránsito y después a VPC D.



Recursos

Cree los siguientes recursos para este escenario:

- Cuatro VPC Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
- Una puerta de enlace de tránsito. Para obtener más información, consulte Crear una puerta de enlace de tránsito.
- Tres conexiones en la puerta de enlace de tránsito, una por VPC. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
- Un adjunto de Site-to-Site VPN en la puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una vinculación de la puerta de enlace de tránsito a una VPN”.

Asegúrese de revisar los requisitos para su dispositivo de puerta de enlace de cliente en la Guía del usuario de AWS Site-to-Site VPN .

Cuando la conexión de VPN se activa, se establece la sesión de BGP y el CIDR de VPN se propaga a la tabla de enrutamiento de puerta de enlace de tránsito y los CIDR de la VPC se agregan a la tabla de BGP de la puerta de enlace de cliente.

- Cada VPC aislada se asocia a la tabla de enrutamiento aislada y se propaga a la tabla de enrutamiento compartida.
- Cada VPC de servicios compartidos aislada se asocia a la tabla de enrutamiento compartida y se propaga a ambas tablas de enrutamiento.

Enrutamiento

Cada VPC tiene una tabla de enrutamiento y la puerta de enlace de tránsito tiene dos tablas de enrutamiento: una para las VPC y otra para la conexión de VPN y servicios compartidos de VPC.

Tablas de enrutamiento de VPC A, VPC B, VPC C y VPC D

Cada VPC tiene una tabla de enrutamiento con 2 entradas. La primera fila es la entrada predeterminada para el direccionamiento local de la VPC. Esta entrada permite a las instancias de esta VPC comunicarse entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la puerta de enlace de tránsito.

Destino	Target
10.1.0. 0/16	local
0.0.0. 0/0	*transit gateway ID*

Tablas de enrutamiento de la puerta de enlace de tránsito

Este escenario utiliza una tabla de enrutamiento para las VPC y una tabla de enrutamiento para la conexión de VPN.

Las vinculaciones de la VPC A, B y C se asocian con la siguiente tabla de ruteo, que tiene una ruta propagada para la vinculación de VPN y una ruta propagada para la vinculación de VPC D.

Destino	Objetivo	Tipo de ruta
10.99,99. 0/24	*Attachment for VPN connection*	propagada
10.4.0. 0/16	*Attachment for VPC D*	propagada

Los adjuntos de VPN y los adjuntos de VPC (VPC D) de servicios compartidos están asociados a la siguiente tabla de enrutamiento, que tiene entradas que apuntan a cada uno de los adjuntos de VPC. Esto permite la comunicación con las VPC desde la conexión VPN y la VPC de servicios compartidos.

Destino	Objetivo	Tipo de ruta
10.1.0. 0/16	*Attachment for VPC A*	propagada
10.2.0. 0/16	*Attachment for VPC B*	propagada
10.3.0. 0/16	*Attachment for VPC C*	propagada

Para obtener más información, consulte Habilitar la propagación de rutas a una tabla de rutas de Transit Gateway en AWS Transit Gateway.

Tabla del BGP de la puerta de enlace de cliente

La tabla BGP de la puerta de enlace de cliente contiene los siguientes CIDR de VPC.

Ejemplo: gateways de tránsito interconectadas

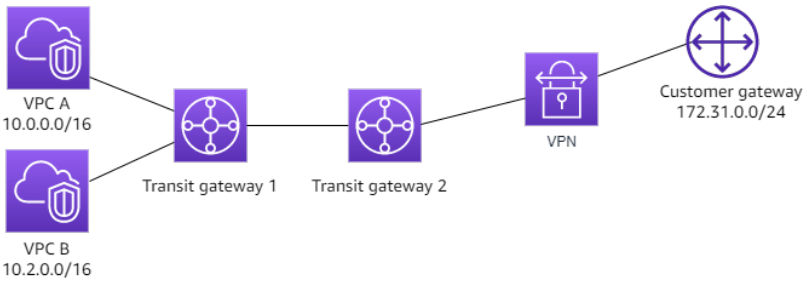
Puede crear una interconexión de puerta de enlace de tránsito entre puertas de enlace de tránsito. A continuación puede dirigir el tráfico entre las vinculaciones de cada una de las gateways de tránsito. En este escenario, las vinculaciones de VPC y VPN se asocian a las tablas de ruteo predeterminadas de la gateway de tránsito y se propagan a las tablas de ruteo predeterminadas de la gateway de tránsito. Cada tabla de ruteo de la gateway de tránsito tiene una ruta estática que apunta a la vinculación de interconexión de gateways de tránsito.

Contenido

- Descripción general de
- Recursos
- Enrutamiento

Descripción general de

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. La pasarela de tránsito 1 tiene dos adjuntos de VPC y la puerta de enlace de tránsito 2 tiene un adjunto de Site-to-Site VPN. Los paquetes de las subredes en VPC A y VPC B que tienen Internet como destino se enrutan primero a través de la gateway de tránsito 1, después a través de la gateway de tránsito 2 y, a continuación, a la conexión de VPN.



Recursos

Cree los siguientes recursos para este escenario:

- Dos VPC. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
- Dos puertas de enlace de tránsito. Pueden estar en la misma región o en regiones diferentes. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
- Dos conexiones de VPC en la primera gateway de tránsito. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
- Un adjunto de Site-to-Site VPN en la segunda puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una vinculación de la puerta de enlace de tránsito a una VPN”. Asegúrese de revisar los requisitos para su dispositivo de gateway de cliente en la Guía del usuario de AWS Site-to-Site VPN .
- Una conexión de interconexión de gateway de tránsito entre las dos gateways de tránsito. Para obtener más información, consulte Vinculaciones de interconexiones de la puerta de enlace de tránsito en AWS Transit Gateway.

Al crear conexiones de VPC, los CIDR de cada VPC se propagan a la tabla de enrutamiento de la gateway de tránsito 1. Cuando la conexión de VPN se activa, se producen las siguientes acciones:

- La sesión del BGP está establecida
- El CIDR de la Site-to-Site VPN se propaga a la tabla de rutas de la pasarela de tránsito 2
- Los CIDR de VPC se agregan a la tabla BGP de la gateway de cliente

Enrutamiento

Cada VPC tiene una tabla de enrutamiento y cada gateway de tránsito tiene una tabla de enrutamiento.

Tablas de enrutamiento de VPC A y VPC B

Cada VPC tiene una tabla de ruteo con 2 entradas. La primera fila es la entrada predeterminada para el direccionamiento IPv4 local de la VPC. Esta entrada predeterminada permite que los recursos de esta VPC se comuniquen entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la gateway de tránsito. La siguiente table muestra las rutas de VPC A.

Destino	Target
10.0.0. 0/16	local
0.0.0. 0/0	tgw-1-id

Tablas de enrutamiento de la gateway de tránsito

A continuación se muestra un ejemplo de la tabla de ruteo predeterminada de la gateway de tránsito 1, con la propagación de rutas habilitada.

Destino	Objetivo	Tipo de ruta
10.0.0. 0/16	*Attachment ID for VPC A*	propagada

Destino	Objetivo	Tipo de ruta
10.2.0. 0/16	*Attachment ID for VPC B*	propagada
0.0.0. 0/0	*Attachment ID for peering connection*	estático

A continuación se muestra un ejemplo de la tabla de ruteo predeterminada de la gateway de tránsito 2, con la propagación de rutas habilitada.

Destino	Objetivo	Tipo de ruta
172,31,0. 0/24	*Attachment ID for VPN connection*	propagada
10.0.0. 0/16	*Attachment ID for peering connection*	estática
10.2.0. 0/16	*Attachment ID for peering connection*	estática

Tabla del BGP de la gateway de cliente

La tabla del número de sistema autónomo de la puerta de enlace de cliente contiene los siguientes CIDR de VPC.

- 10.0.0. 0/16
- 10.2.0. 0/16

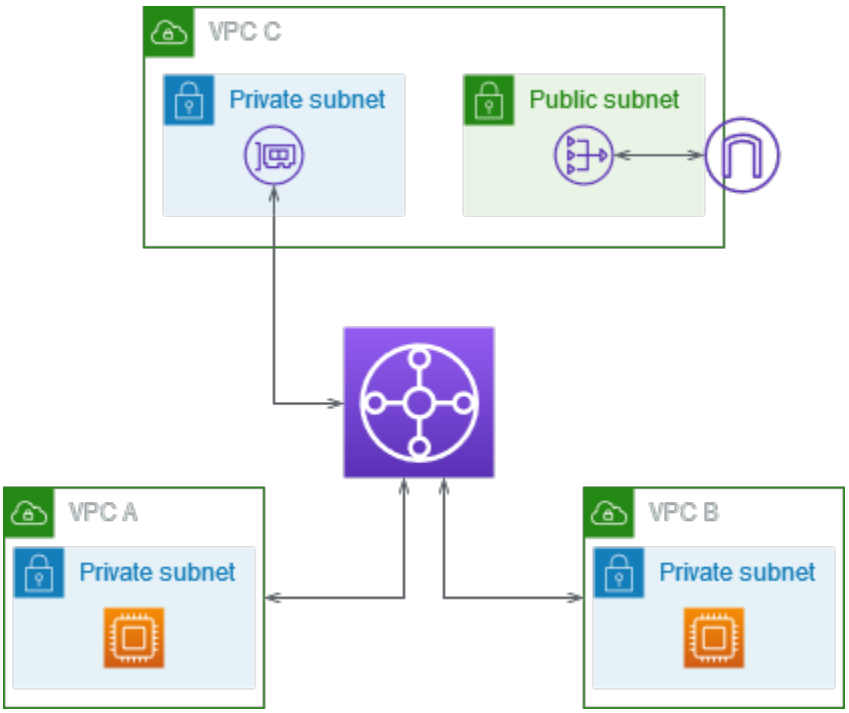
Ejemplo: enrutamiento saliente centralizado a Internet

Puede configurar una puerta de enlace de tránsito para dirigir el tráfico de Internet saliente desde una VPC sin puerta de enlace de Internet a una VPC que contenga una puerta de enlace NAT y una puerta de enlace de Internet.

Contenido

Descripción general de

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. Tiene aplicaciones en la VPC A y la VPC B que solo necesitan acceso saliente a Internet. Configure la VPC C con una puerta de enlace NAT pública y una puerta de enlace de Internet y una subred privada para la conexión a la VPC. Conecte todas las VPC a una puerta de enlace de tránsito. Configure el enrutamiento para que el tráfico de Internet saliente de la VPC A y la VPC B atraviese la puerta de enlace de tránsito a la VPC C. La puerta de enlace NAT en la VPC C dirige el tráfico a la puerta de enlace de Internet.



Recursos

Cree los siguientes recursos para este escenario:

- Tres VPC con rangos de direcciones IP que no son idénticos ni se superponen. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
- La VPC A y la VPC B tienen subredes privadas con instancias EC2.
- La VPC C tiene lo siguiente:

  - Una puerta de enlace de Internet adjuntada a la VPC. Para obtener más información, consulte Crear y adjuntar una puerta de enlace de Internet en la Guía del usuario de Amazon VPC.
  - Una subred pública con una puerta de enlace NAT. Para obtener información, consulte Creación de una puerta de enlace NAT en la Guía del usuario de Amazon VPC.
  - Una subred en VPC C para la conexión de puerta de enlace de tránsito. La subred privada debe estar en la misma zona de disponibilidad que la subred pública.
- Una puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
- Tres conexiones de VPC en la puerta de enlace de tránsito. Los bloques de CIDR de cada VPC se propagan a la tabla de enrutamiento de la gateway de tránsito. Para obtener más información, consulte the section called “Crear una conexión de VPC”. Para la VPC C, debe crear la conexión mediante la subred privada. Si crea la conexión mediante la subred pública, el tráfico de la instancia se enruta a la puerta de enlace de Internet, pero la puerta de enlace de Internet reduce el tráfico porque las instancias no tienen direcciones IP públicas. Al colocar la conexión en la subred privada, el tráfico se enruta a la puerta de enlace NAT y la puerta de enlace NAT envía tráfico a la puerta de enlace de Internet usando una dirección IP elástica como la dirección IP de origen.

Enrutamiento

Hay tablas de enrutamiento para cada VPC y una tabla de enrutamiento para la puerta de enlace de tránsito.

Tablas de ruteo

- Tabla de enrutamiento para la VPC A
- Tabla de enrutamiento para la VPC B
- Tablas de enrutamiento para VPC C
- Tabla de enrutamiento de la puerta de enlace de tránsito

Tabla de enrutamiento para la VPC A

A continuación, se muestra una tabla de enrutamiento de ejemplo. La primera entrada habilita a las instancias de la VPC a comunicarse entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la gateway de tránsito.

Destino	Objetivo
VPC A CIDR	local
0.0.0. 0/0	*transit-gateway-id*

Tabla de enrutamiento para la VPC B

A continuación, se muestra una tabla de enrutamiento de ejemplo. La primera entrada habilita a las instancias de la VPC a comunicarse entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la gateway de tránsito.

Destino	Objetivo
VPC B CIDR	local
0.0.0. 0/0	*transit-gateway-id*

Tablas de enrutamiento para VPC C

Configure la subred con la puerta de enlace NAT como una subred pública agregando una ruta a la puerta de enlace de Internet. Mantenga la otra subred como una subred privada.

A continuación, se muestra una tabla de enrutamiento de ejemplo para la subred pública. La primera entrada habilita a las instancias de la VPC a comunicarse entre sí. La segunda entrada y la tercera entrada dirigen el tráfico de la VPC A y la VPC B a la puerta de enlace de tránsito. Las demás entradas dirigen el resto del tráfico de la subred de IPv4 a la puerta de enlace de Internet.

Destino	Objetivo
VPC C CIDR	local
VPC A CIDR	*transit-gateway-id*
VPC B CIDR	*transit-gateway-id*

Destino	Objetivo
0.0.0. 0/0	*internet-gateway-id*

A continuación, se muestra una tabla de enrutamiento de ejemplo para la subred privada. La primera entrada habilita a las instancias de la VPC a comunicarse entre sí. La segunda entrada dirige el resto del tráfico de la subred de IPv4 a la puerta de enlace NAT.

Destino	Objetivo
VPC C CIDR	local
0.0.0. 0/0	*nat-gateway-id*

Tabla de enrutamiento de la puerta de enlace de tránsito

A continuación se muestra un ejemplo de la tabla de enrutamiento de la puerta de enlace de tránsito. Los bloques de CIDR de cada VPC se propagan a la tabla de enrutamiento de la gateway de tránsito. La ruta estática envía tráfico de Internet saliente a la VPC C. Puede evitar la comunicación entre las VPC agregando una ruta de agujero negro para cada CIDR de VPC.

CIDR	Conexión	Tipo de ruta
VPC A CIDR	*Attachment for VPC A*	propagada
VPC B CIDR	*Attachment for VPC B*	propagada
VPC C CIDR	*Attachment for VPC C*	propagada
0.0.0. 0/0	*Attachment for VPC C*	estática

Ejemplo: Dispositivo en una VPC de servicios compartidos

Puede configurar un dispositivo (como un dispositivo de seguridad) en una VPC de servicios compartidos. Todo el tráfico enrutado entre la puerta de enlaces de tránsito lo inspecciona primero el dispositivo en la VPC de servicios compartidos. Cuando se habilita el modo de dispositivo, una puerta de enlace de tránsito selecciona una única interfaz de red en la VPC del dispositivo, mediante un algoritmo hash de flujo, para enviar tráfico a lo largo de la vida útil del flujo. La puerta de enlace de tránsito utiliza la misma interfaz de red para el tráfico de retorno. Esto garantiza que el tráfico bidireccional se enrute simétricamente: se enruta a través de la misma zona de disponibilidad en la conexión de VPC durante el tiempo de vida del flujo. Si tiene varias puertas de enlace de tránsito en su arquitectura, cada puerta de enlace de tránsito mantiene su propia afinidad de sesión y cada puerta de enlace de tránsito puede seleccionar una interfaz de red diferente.

Debe conectar exactamente una puerta de enlace de tránsito a la VPC del dispositivo para garantizar la adherencia del flujo. La conexión de varias puertas de enlace de tránsito a una sola VPC del dispositivo no garantiza la adherencia del flujo porque las puertas de enlace de tránsito no comparten información de estado de flujo entre sí.

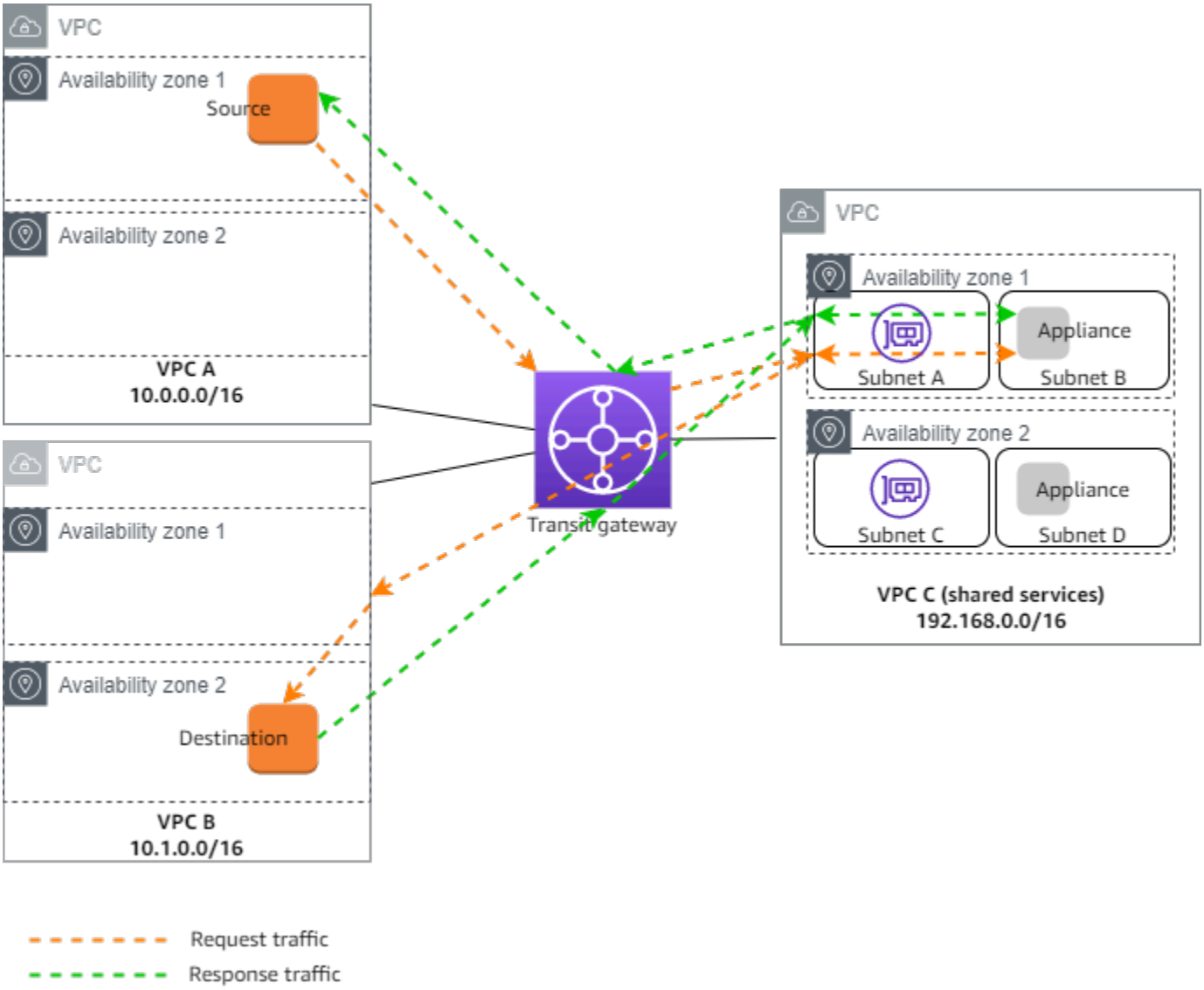
Important

- El tráfico en modo dispositivo se enruta correctamente siempre que el tráfico de origen y de destino llegue a una VPC centralizada (VPC de inspección) desde la misma conexión de puerta de enlace de tránsito. El tráfico puede disminuir si el origen y el destino están en dos conexiones de puerta de enlace de tránsito diferentes. El tráfico puede disminuir si la VPC centralizada recibe el tráfico de una puerta de enlace diferente (por ejemplo, de una puerta de enlace de Internet) y luego envía ese tráfico a la conexión de puerta de enlace de tránsito tras la inspección.
- La activación del modo dispositivo en una conexión existente puede afectar a la ruta actual de esa conexión, ya que esta puede fluir a través de cualquier zona de disponibilidad. Cuando el modo dispositivo no está habilitado, el tráfico se mantiene hacia la zona de disponibilidad de origen.

Contenido

Descripción general de

El siguiente diagrama muestra los componentes clave de la configuración de este escenario. La puerta de enlace de tránsito tiene tres conexiones de VPC. VPC C es una VPC de servicios compartidos. El tráfico entre VPC A y VPC B se enruta a la puerta de enlace de tránsito y, a continuación, se enruta a un dispositivo de seguridad en VPC C para su inspección antes de que se enrute al destino final. El dispositivo es un dispositivo con estado, por lo que se inspecciona el tráfico de solicitud como el de respuesta. Para una alta disponibilidad, hay un dispositivo en cada zona de disponibilidad de VPC C.



Cree los siguientes recursos para este escenario:

- Tres VPC Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.

- Una puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
- Tres conexiones de VPC: una para cada una de las VPC. Para obtener más información, consulte the section called “Crear una conexión de VPC”.

  Para cada conexión de VPC, especifique una subred en cada zona de disponibilidad. Para la VPC de servicios compartidos, estas son las subredes donde el tráfico se enruta a la VPC desde la puerta de enlace de tránsito. En el ejemplo anterior, se trata de subredes A y C.

  Para las conexiones de VPC para VPC C, habilite la compatibilidad con el modo de dispositivo para que el tráfico de respuesta se enrute a la misma zona de disponibilidad en VPC C que el tráfico de origen.

  La consola de Amazon VPC admite el modo de dispositivo. También puede utilizar la API de Amazon VPC, un AWS SDK, el modo AWS CLI para habilitar el dispositivo o. CloudFormation Por ejemplo, agregue `--options ApplianceModeSupport=enable` al comando create-transit-gateway-vpc-attachment o modify-transit-gateway-vpc-attachment.

> **Note**
>
> La rigidez del flujo en el modo de dispositivo solo está garantizada para el tráfico de origen y destino que se dirige a la VPC de inspección.

Dispositivos con estado y modo de dispositivo

Si las conexiones de VPC abarcan varias zonas de disponibilidad y necesita que el tráfico entre hosts de origen y destino se enrute a través del mismo dispositivo para una inspección con estado, habilite la compatibilidad con el modo de dispositivo para la conexión de VPC en que se encuentra el dispositivo.

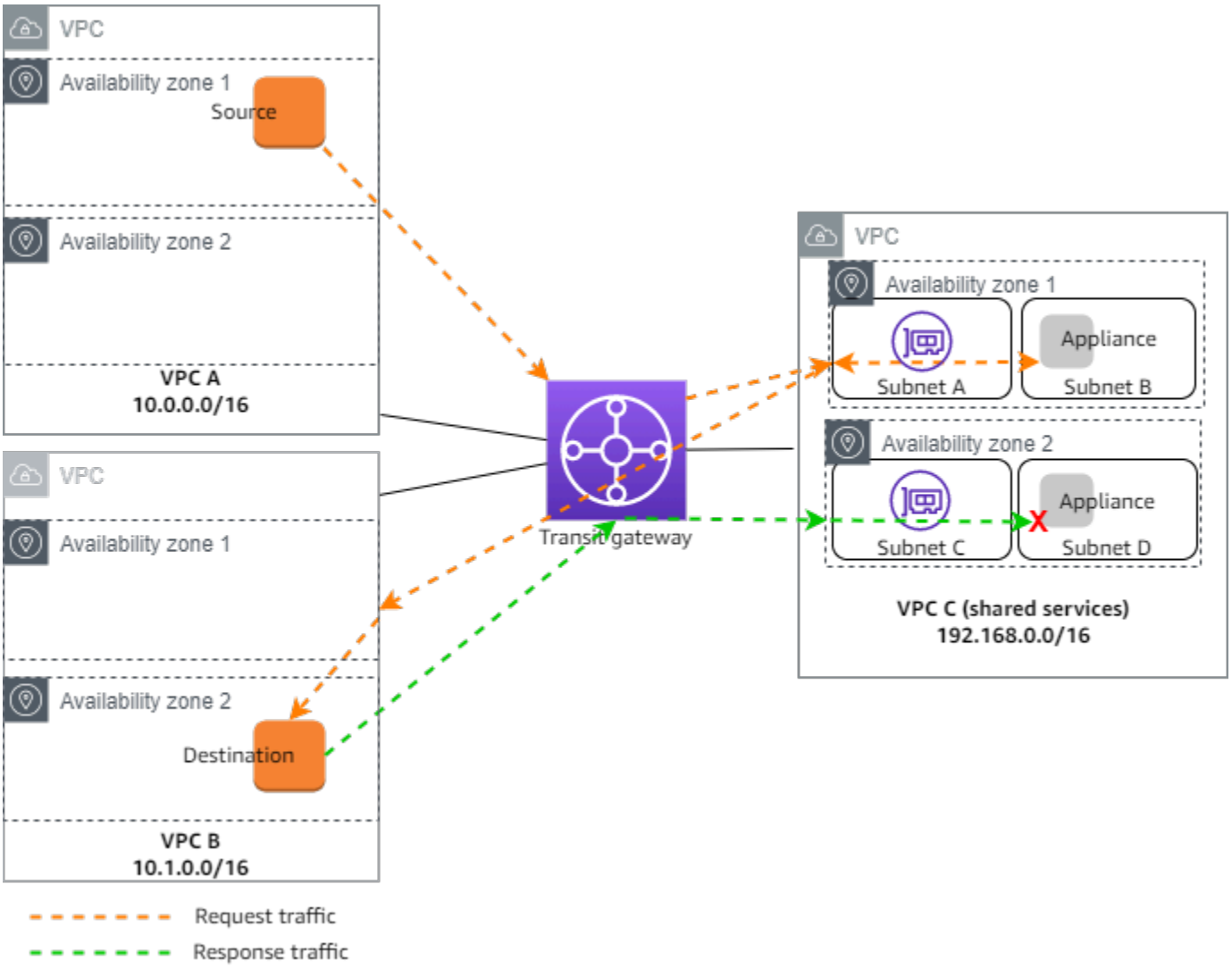
Para obtener más información, consulte Arquitectura de inspección centralizada en el AWS blog.

Comportamiento cuando el modo de dispositivo no está habilitado

Cuando el modo de dispositivo no está habilitado, una puerta de enlace de tránsito intenta mantener el tráfico enrutado entre las conexiones de la VPC en la zona de disponibilidad de origen hasta que llegue a su destino. El tráfico cruza zonas de disponibilidad entre conexiones solo si se produce un

error en la zona de disponibilidad o si no hay subredes asociadas con una conexión de VPC en esa zona de disponibilidad.

El siguiente diagrama muestra un flujo de tráfico cuando la compatibilidad con el modo de dispositivo no está habilitada. El tráfico de respuesta que se origina en la zona de disponibilidad 2 de la VPC B se enruta por la puerta de enlace de tránsito a la misma zona de disponibilidad en VPC C. Por lo tanto, el tráfico se elimina porque el dispositivo de la zona de disponibilidad 2 no conoce la solicitud original del origen en VPC A.



Enrutamiento

Cada VPC tiene una o varias tablas de enrutamiento y la puerta de enlace de tránsito tiene dos tablas de enrutamiento.

Tablas de enrutamiento de la VPC

VPC A y VPC B

VPC A y B tienen tablas de enrutamiento con 2 entradas. La primera fila es la entrada predeterminada para el direccionamiento IPv4 local de la VPC. Esta entrada predeterminada permite que los recursos de esta VPC se comuniquen entre sí. La segunda entrada enruta el resto del tráfico de subredes de IPv4 a la puerta de enlace de tránsito. A continuación, se muestra la tabla de enrutamiento para VPC A.

Destino	Target
10.0.0. 0/16	local
0.0.0. 0/0	tgw-id

VPC C

La VPC de servicios compartidos (VPC C) tiene tablas de enrutamiento diferentes para cada subred. La puerta de enlace de tránsito utiliza la subred A (debe especificar esta subred al crear la conexión de VPC). La tabla de enrutamiento de la subred A enruta todo el tráfico al dispositivo de la subred B.

Destino	Target
192.168.0. 0/16	local
0.0.0. 0/0	appliance-eni-id

La tabla de enrutamiento de la subred B (que contiene el dispositivo) enruta el tráfico de vuelta a la puerta de enlace de tránsito.

Destino	Target
192.168.0. 0/16	local
0.0.0. 0/0	tgw-id

Tablas de enrutamiento de la puerta de enlace de tránsito

Esta puerta de enlace de tránsito utiliza una tabla de enrutamiento para VPC A y VPC B y una tabla de enrutamiento para la VPC de servicios compartidos (VPC C).

Las conexiones de VPC A y VPC B se asocian con la siguiente tabla de enrutamiento. La tabla de enrutamiento enruta todo el tráfico a VPC C.

Destino	Objetivo	Tipo de ruta
0.0.0. 0/0	*Attachment ID for VPC C*	estática

La conexión de VPC C se asocia con la siguiente tabla de enrutamiento. Enruta el tráfico a VPC A y VPC B.

Destino	Objetivo	Tipo de ruta
10.0.0. 0/16	*Attachment ID for VPC A*	propagada
10.1.0. 0/16	*Attachment ID for VPC B*	propagada

Tutoriales: introducción a AWS Transit Gateway

Los siguientes tutoriales lo ayudan a familiarizarse con las puertas de enlace de tránsito en AWS Transit Gateway. Las tareas incluidas en los siguientes tutoriales le ayudarán a crear una puerta de enlace de tránsito y luego a conectar dos VPC con esa puerta de enlace de tránsito. Puede crear una puerta de enlace de tránsito mediante la consola de Amazon VPC o la AWS CLI.

Tareas

- Tutorial: crear una AWS Transit Gateway mediante la consola de Amazon VPC
- Tutorial: Crear una AWS Transit Gateway mediante la línea de AWS comandos

Tutorial: crear una AWS Transit Gateway mediante la consola de Amazon VPC

En este tutorial, aprenderá a usar la consola de Amazon VPC para crear una puerta de enlace de tránsito y conectarle dos VPC. Creará la puerta de enlace de tránsito, conectará las dos VPC y, a continuación, configurará las rutas necesarias para permitir la comunicación entre la puerta de enlace de tránsito y sus VPC.

Requisitos previos

- Para mostrar un ejemplo sencillo de cómo usar una gateway de tránsito, cree dos VPC en la misma región. Las VPC no pueden tener CIDR idénticos ni superpuestos. Lance una instancia Amazon EC2 en cada VPC. Para obtener más información, consulte Creación de una VPC en la Guía del usuario de Amazon VPC y Lanzamiento de una instancia en la Guía del usuario de Amazon EC2.
- No se pueden tener rutas idénticas que señalen a dos VPC distintas. Una gateway de tránsito no propaga los CIDRs de una VPC recién asociada si existe una ruta idéntica en las tablas de enrutamiento de la gateway de tránsito.
- Compruebe que tiene los permisos necesarios para trabajar con gateways de tránsito. Para obtener más información, consulte Gestión de identidad y acceso en AWS Transit Gateway.
- No puede hacer ping entre hosts si no ha agregado una regla ICMP a cada uno de los grupos de seguridad del host. Para obtener más información, consulte Configuración de reglas del grupo de seguridad en la Guía del usuario de Amazon VPC

Pasos

Paso 1: Crear la gateway de tránsito

Cuando crea una gateway de tránsito, se crea una tabla de ruteo de la gateway de tránsito predeterminada y se utiliza como tabla de ruteo de asociación y de propagación predeterminada.

Para crear una gateway de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el selector de regiones, elija la región que utilizó al crear las VPC.
3. En el panel de navegación, elija Transit Gateways (Gateways de tránsito).
4. Elija Create Transit Gateway (Crear gateway de tránsito).
5. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la gateway de tránsito. Al hacerlo, se crea una etiqueta con "Name (Nombre)" como clave y el nombre que especificó como valor.
6. (Opcional) En Description (Descripción), ingrese una descripción para la gateway de tránsito.
7. En la sección Configurar la puerta de enlace de tránsito, haga lo siguiente:

    1. En Amazon side Autonomous System Number (ASN) (Número de sistema autónomo (ASN) del lado de Amazon), ingrese el ASN privado de la gateway de tránsito. Este debe ser el ASN para el lado AWS de una sesión de protocolo de gateway fronteriza (BGP).

        El rango va de 64512 a 65534 para los ASN de 16 bits.

        El rango va de 4200000000 a 4294967294 para los ASN de 32 bits.

        Si tiene una implementación en varias regiones, recomendamos que utilice un ASN único para cada una de las puerta de enlaces de tránsito.
    2. (Opcional) Seleccione si desea habilitar una de las siguientes opciones:
        - Compatibilidad con DNS para las VPC conectadas a esta puerta de enlace de tránsito.

- Compatibilidad con VPN ECMP para las conexiones de VPN vinculadas a la puerta de enlace de tránsito.
- Asociación de tabla de enrutamiento predeterminada, la cual asocia automáticamente las conexiones de puerta de enlace de tránsito a la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito.
- Propagación de tablas de enrutamiento predeterminada, la cual propaga automáticamente las conexiones de la tabla de enrutamiento a la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito.
- Compatibilidad con multidifusión, la cual permite crear dominios de multidifusión en esta puerta de enlace de tránsito.

8. (Opcional) En la sección Opciones de configuración del uso compartido entre cuentas, marque o desmarque Aceptar automáticamente las conexiones compartidas. Si la opción está habilitada, las conexiones se aceptan automáticamente. De lo contrario, debe aceptar o rechazar las solicitudes de conexión.
9. (Opcional) En la sección de bloques CIDR de la puerta de enlace de tránsito, agregue un bloque CIDR de tamaño /24 o superior para las direcciones IPv4 o un bloque CIDR de /64 o superior para las direcciones IPv6. Puede asociar cualquier rango de direcciones IP públicas o privadas, excepto las direcciones del rango 169.254.0.0/16 y los rangos que se superponen con las direcciones de las vinculaciones de VPC y las redes en las instalaciones.

   > **Note**
   >
   > Los bloques CIDR de la puerta de enlace de tránsito se utilizan si configura conexiones de Connect (GRE) o VPN con IP privada. Transit Gateway asigna direcciones IP a los puntos de conexión del túnel (GRE/VPN con IP privada) de este rango.

10. (Opcional) Agregue etiquetas clave-valor a esta puerta de enlace de tránsito para identificarla aún más.
    1. Elija Añadir nueva etiqueta.
    2. Introduzca un nombre de clave y un valor asociado.
    3. Seleccione Agregar nueva etiqueta para agregar etiquetas adicionales o avance al siguiente paso.
11. Elija Create Transit Gateway (Crear gateway de tránsito). Cuando se crea la gateway, el estado inicial de la gateway de tránsito es `pending`.

Paso 2: Adjuntar las VPC a las gateways de tránsito

Espere hasta que la gateway de tránsito que ha creado en la sección anterior se muestre como disponible antes de continuar con la creación de una conexión. Cree una vinculación para cada VPC.

Confirme que ha creado dos VPC y que ha lanzado una instancia EC2 en cada una de ellas, como se describe en Requisitos previos.

Crear una vinculación de la gateway de tránsito a una VPC

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Elija Create transit gateway attachment (Crear conexión de gateway de tránsito).
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la conexión.
5. En Transit Gateway ID (ID de gateway de tránsito), elija la gateway de tránsito que se debe utilizar para la conexión.
6. En Attachment type (Tipo de vinculación), elija VPC.
7. Elija si desea habilitar DNS support (Compatibilidad de DNS). Para este ejercicio, no habilite IPv6 support (Compatibilidad con IPv6).
8. En VPC ID (ID de VPC), elija la VPC que desee asociar a la gateway de tránsito.
9. En Subnet IDs (ID de subred), seleccione una subred para cada zona de disponibilidad que la gateway de tránsito utilizará para enrutar el tráfico. Debe seleccionar al menos una subred. Solo puede seleccionar una subred por zona de disponibilidad.
10. Elija Create transit gateway attachment (Crear conexión de gateway de tránsito).

Cada vinculación se asocia siempre a una sola tabla de ruteo. Las tablas de ruteo pueden asociarse con un número de cero a varias vinculaciones. Para determinar las rutas que se van a configurar, decida el caso de uso de la gateway de tránsito y, a continuación, configure las rutas. Para obtener más información, consulte the section called “Ejemplos de escenarios de la puerta de enlace de tránsito”.

Paso 3: Agregar rutas entre la gateway de tránsito y las VPC

Una tabla de ruteo incluye rutas dinámicas y estáticas que determinan el siguiente salto para las VPC asociadas en función de la dirección IP de destino del paquete. Configure una ruta que tenga un

destino para rutas no locales y el destino del ID de la conexión de gateway de tránsito. Para obtener más información, consulte Direccionamiento para una gateway de tránsito en la Guía del usuario de Amazon VPC.

Para añadir una ruta a una tabla de ruteo de VPC

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).
3. Elija la tabla de ruteo asociada a su VPC.
4. Elija la pestaña Routes (Rutas) y, a continuación, Edit routes (Editar rutas).
5. Seleccione Add route (Añadir ruta).
6. Introduzca el rango de direcciones IP de destino en la columna Destination (Destino). Para Target (Objetivo), elija Transit Gateway (Puerta de enlace de tránsito) y, a continuación, elija el ID de la puerta de enlace de tránsito.
7. Seleccione Save changes (Guardar cambios).

Paso 4: Pruebe la gateway de tránsito

Puede confirmar que la gateway de tránsito se ha creado correctamente al conectarse a una instancia Amazon EC2 en cada VPC y, a continuación, enviar datos entre ellas, como un comando ping. Para obtener más información, consulte Conexión con instancias EC2 en la Guía del usuario de Amazon EC2.

Paso 5: Eliminar la gateway de tránsito

Cuando ya no necesite una gateway de tránsito, puede eliminarla.

No se puede eliminar una gateway de tránsito que tenga conexiones de recursos. Si intenta eliminar una puerta de enlace de tránsito con archivos adjuntos, se le pedirá que primero elimine esos archivos adjuntos antes de poder eliminar la puerta de enlace de tránsito. En cuanto se elimine la gateway de tránsito, se le dejarán de aplicar cargos por ella.

Para eliminar la gateway de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways (Puertas de enlace de tránsito).

3. Seleccione la puerta de enlace de tránsito y luego elija Actions (Acciones), Delete transit gateway (Eliminar puerta de enlace de tránsito).
4. Ingrese **`delete`** y elija Delete (Eliminar).

   El State (Estado) de la puerta de enlace de tránsito en la página Transit gateways (Puertas de enlace de tránsito) es Deleting (Eliminándose). Una vez eliminada, la puerta de enlace de tránsito se elimina de la página.

Tutorial: Crear una AWS Transit Gateway mediante la línea de AWS comandos

En este tutorial, aprenderás a usar la AWS CLI para crear una pasarela de tránsito y conectar dos VPCs a ella. Creará la pasarela de transporte, conectará ambas y VPCs, a continuación, configurará las rutas necesarias para permitir la comunicación entre la pasarela de transporte y la suya VPCs.

Requisitos previos

Antes de empezar, asegúrese de que tiene lo siguiente:

- AWS CLI instalado y configurado con los permisos adecuados. Si no tiene la AWS CLI instalada, consulte la Documentación de la interfaz de línea de comandos de AWS .
- No VPCs pueden ser idénticos ni superpuestos CIDRs. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
- Una instancia EC2 en cada VPC. Para conocer los pasos para lanzar una instancia EC2 en una VPC, consulteLanzar una instancia en la Guía del usuario de Amazon EC2.
- Grupos de seguridad configurados para permitir el tráfico ICMP entre las instancias. Para conocer los pasos para controlar el tráfico con grupos de seguridad, consulte Controlar el tráfico hacia los recursos de AWS mediante grupos de seguridad en la Guía del usuario de Amazon VPC.
- Permisos de IAM adecuados para trabajar con puertas de enlace de tránsito. Para comprobar los permisos de IAM de Transit Gateways, consulta la sección Gestión de identidad y acceso en AWS Transit Gateways en la AWS Transit Gateway Guía.

Steps

- Paso 1: Crear la gateway de tránsito
- Paso 2: Verificar el estado de disponibilidad de puerta de enlace de tránsito

Paso 1: Crear la gateway de tránsito

Al crear una puerta de enlace de tránsito, AWS crea una tabla de rutas de la puerta de enlace de tránsito predeterminada y la usa como tabla de rutas de asociación predeterminada y tabla de rutas de propagación predeterminada. A continuación se muestra un ejemplo de solicitud de `create-transit-gateway` en la región `us-west-2`. En la solicitud se incluyeron otras `options`. Para obtener más información sobre el `create-transit-gateway` comando, incluida una lista de las opciones que puede incluir en la solicitud, consulte create-transit-gateway.

```
aws ec2 create-transit-gateway \
  --description "My Transit Gateway" \
  --region us-west-2
```

A continuación, la respuesta muestra que se creó la puerta de enlace de tránsito. En la respuesta, las `0ptions` que se devuelven contienen todos valores predeterminados.

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "pending",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
```

```
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        }
    }
}
```

> **Note**
>
> Este comando devuelve información sobre su nueva puerta de enlace de tránsito, incluida la ID. Anote la ID de puerta de enlace de tránsito (`tgw-1234567890abcdef0`), ya que se lo necesitará en los pasos siguientes.

Paso 2: Verificar el estado de disponibilidad de puerta de enlace de tránsito

Cuando se crea una puerta de enlace de tránsito, se coloca en un estado `pending`. El estado pasará de pendiente a disponible automáticamente, pero hasta que no lo haga, no podrá adjuntar ninguno VPCs hasta que cambie el estado. Para verificar el estado, ejecute el comando `describe-transit-gatweways` con la ID de la puerta de enlace de tránsito recién creada junto con la opción de filtros. La opción `filters` usa los pares `Name=state` y `Values=available`. A continuación, el comando busca verificar si el estado de su puerta de enlace de tránsito se encuentra disponible. Si es así, aparecerá la respuesta `"State": "available"`. Si está en cualquier otro estado, entonces aún no está disponible para su uso. Espere unos minutos antes de ejecutar el comando.

Para obtener más información acerca del comando `describe-transit-gateways`, consulte describe-transit-gateways.

```
aws ec2 describe-transit-gateways \
  --transit-gateway-ids tgw-1234567890abcdef0 \
  --filters Name=state,Values=available
```

Espere a que el estado de la puerta de enlace de tránsito cambie de `pending` a `available` antes de continuar. En la siguiente respuesta, el `State` ha cambiado a `available`.

```
{
    "TransitGateways": [
        {
            "TransitGatewayId": "tgw-1234567890abcdef0",
```

```
            "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
            "State": "available",
            "OwnerId": "123456789012",
            "Description": "My Transit Gateway",
            "CreationTime": "2022-04-20T19:58:25+00:00",
            "Options": {
                "AmazonSideAsn": 64512,
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "DefaultRouteTablePropagation": "enable",
                "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "disable",
                "MulticastSupport": "disable"
            },
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "example-transit-gateway"
                }
            ]
        }
    ]
}
```

Paso 3: Adjunta el tuyo VPCs a tu pasarela de transporte

Una vez que esté disponible la puerta de enlace de tránsito, cree un archivo adjunto para cada VPC mediante la `create-transit-gateway-vpc-attachment`. Se deben incluir la `transit-gateway-id`, la `vpc-id` y las `subnet-ids`.

Para obtener más información sobre el `create-transit-vpc attachment` comando, consulte create-transit-gateway-vpc-attachment.

En el siguiente ejemplo, el comando se ejecuta dos veces, una para cada VPC.

Para la primera VPC, ejecute lo siguiente con la primera `vpc_id` y las `subnet-ids`

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
```

```
  --vpc-id vpc-1234567890abcdef0 \
  --subnet-ids subnet-1234567890abcdef0
```

La respuesta muestra que la vinculación se realizó correctamente. La vinculación se crea en un estado `pending`. No es necesario cambiar este estado, ya que pasa a ser un estado `available` de manera automática. Esto podría tardar varios minutos.


```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-1234567890abcdef0",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-1234567890abcdef0",
            "subnet-abcdef1234567890"
        ],
        "CreationTime": "2025-06-23T18:35:11+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```


Para la segunda VPC, ejecute el mismo comando anterior con la segunda `vpc_id` y las `subnet-ids`:

```
aws ec2 create-transit-gateway-vpc-attachment \
  --transit-gateway-id tgw-1234567890abcdef0 \
  --vpc-id vpc-abcdef1234567890 \
  --subnet-ids subnet-abcdef01234567890
```

La respuesta a este comando también muestra una vinculación correcta, con la vinculación actualmente en un estado `pending`.


```
{
    {
    "TransitGatewayVpcAttachment": {
```

```
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "pending",
        "SubnetIds": [
            "subnet-fedcba0987654321",
            "subnet-0987654321fedcba"
        ],
        "CreationTime": "2025-06-23T18:42:56+00:00",
        "Options": {
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "enable",
            "Ipv6Support": "disable",
            "ApplianceModeSupport": "disable"
        }
    }
}
```

Paso 4: Comprobar que las conexiones de puerta de enlace de tránsito estén disponibles

Las conexiones de puerta de enlace de tránsito se crean en un estado `pending` inicial. No podrá usar estas conexiones en sus rutas hasta que el estado cambie a `available`. Esto se produce automáticamente. Utilice el comando `describe-transit-gateways`, junto con la `transit-gateway-id`, para comprobar el `State`. Para obtener más información acerca del comando `describe-transit-gateways`, consulte describe-transit-gateways.

Ejecute el siguiente comando para comprobar el estado. En este ejemplo, los campos de filtro opcionales `Name` y `Values` se envían dentro de la solicitud:

```
aws ec2 describe-transit-gateway-vpc-attachments \
  --filters Name=transit-gateway-id,Values=tgw-1234567890abcdef0
```

La siguiente respuesta muestra que ambas vinculaciones están en un estado `available`:

```
{
    "TransitGatewayVpcAttachments": [
        {
            "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
            "TransitGatewayId": "tgw-1234567890abcdef0",
```

```
            "VpcId": "vpc-1234567890abcdef0",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-1234567890abcdef0",
                "subnet-abcdef1234567890"
            ],
            "CreationTime": "2025-06-23T18:35:11+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        },
        {
            "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
            "TransitGatewayId": "tgw-1234567890abcdef0",
            "VpcId": "vpc-abcdef1234567890",
            "VpcOwnerId": "123456789012",
            "State": "available",
            "SubnetIds": [
                "subnet-fedcba0987654321",
                "subnet-0987654321fedcba"
            ],
            "CreationTime": "2025-06-23T18:42:56+00:00",
            "Options": {
                "DnsSupport": "enable",
                "SecurityGroupReferencingSupport": "enable",
                "Ipv6Support": "disable",
                "ApplianceModeSupport": "disable"
            },
            "Tags": []
        }
    ]
}
```


Paso 5: Agrega rutas entre tu pasarela de tránsito y VPCs

Configure las rutas en la tabla de enrutamiento de cada VPC para dirigir el tráfico a la otra VPC a través de la puerta de enlace de tránsito mediante el comando `create-route` junto con la `transit-gateway-id` para cada tabla de enrutamiento de VPC. En el siguiente ejemplo, el

comando se ejecuta dos veces, una para cada VPC tabla de enrutamiento. La solicitud incluye la `route-table-id`, el `destination-cidr-block` y la `transit-gateway-id` para cada ruta de VPC que esté creando.

Para obtener más información acerca del comando `create-route`, consulte create-route.

Para la tabla de enrutamiento de la primera VPC, ejecute el siguiente comando:

```
aws ec2 create-route \
  --route-table-id rtb-1234567890abcdef0 \
  --destination-cidr-block 10.2.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

Para la tabla de enrutamiento de la segunda VPC, ejecute el siguiente comando: Esta ruta utiliza una `route-table-id` y un `destination-cidr-block` diferente de la primera VPC. Sin embargo, dado que solo utiliza una única puerta de enlace de tránsito, se utiliza la misma `transit-gateway-id`.

```
aws ec2 create-route \
  --route-table-id rtb-abcdef1234567890 \
  --destination-cidr-block 10.1.0.0/16 \
  --transit-gateway-id tgw-1234567890abcdef0
```

La respuesta devuelve `true` para cada ruta e indica que las rutas se crearon.

```
{
    "Return": true
}
```

> **Note**
>
> Sustituya los bloques CIDR de destino por los bloques CIDR reales de su. VPCs

Paso 6: Pruebe la puerta de enlace de tránsito

Se puede confirmar que la puerta de enlace de tránsito se ha creado correctamente al conectarse a una instancia EC2 en una VPC y hacer ping a una instancia en la otra VPC y, a continuación, ejecutar el comando `ping`.

1. Conectarse a la instancia de EC2 en la primera VPC mediante SSH o EC2 Instance Connect
2. Haga ping a la dirección IP privada de la instancia EC2 en la segunda VPC:

```
ping 10.2.0.50
```

> **Note**
>
> Sustituya `10.2.0.50` por la dirección IP privada real de la instancia de EC2 en la segunda VPC.

Si el ping se realiza correctamente, su puerta de enlace de tránsito está configurada correctamente y redirige el tráfico entre las suyas VPCs.

Paso 7: Elimine las conexiones de puerta de enlace de tránsito y la puerta de enlace de tránsito

Cuando ya no necesite una puerta de enlace de tránsito, puede eliminarla. En primer lugar, debe eliminar todas las vinculaciones (conexiones) Ejecute el comando `delete-transit-gateway-vpc-attachment` con la `transit-gateway-attachment-id` para cada vinculación. Después de ejecutar el comando, utilice `delete-transit-gateway` para eliminar la puerta de enlace de tránsito. Para lo siguiente, elimine las dos vinculaciones de VPC y la puerta de enlace de tránsito única que se crearon en los pasos anteriores.

> **Important**
>
> Ya no incurrirá en cargos una vez que elimine todas las conexiones de puerta de enlace de tránsito.

1. Elimine las vinculaciones de VPC mediante el comando `delete-transit-gateway-vpc-attachment`. Para obtener más información sobre `delete-transit-gateway-vpc-attachment` el comando, consulte delete-transit-gateway-vpc-attachment.

   Para la primera vinculación, ejecute el comando siguiente:

```
aws ec2 delete-transit-gateway-vpc-attachment \
```

```
  --transit-gateway-attachment-id tgw-attach-1234567890abcdef0
```

La respuesta de eliminación para la primera vinculación de la VPC devuelve lo siguiente:

```
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-1234567890abcdef0",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

Ejecute el comando `delete-transit-gateway-vpc-attachment` para la segunda vinculación:

```
aws ec2 delete-transit-gateway-vpc-attachment \
  --transit-gateway-attachment-id tgw-attach-abcdef1234567890
```

La respuesta de eliminación para la segunda vinculación de la VPC devuelve lo siguiente:

```
The response returns:
{
    "TransitGatewayVpcAttachment": {
        "TransitGatewayAttachmentId": "tgw-attach-abcdef1234567890",
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "VpcId": "vpc-abcdef1234567890",
        "VpcOwnerId": "123456789012",
        "State": "deleting",
        "CreationTime": "2025-06-23T18:42:56+00:00"
    }
}
```

2. Las vinculaciones están en un estado `deleting` hasta que se eliminan. Una vez eliminadas, se puede eliminar la puerta de enlace de tránsito. Utilice el comando `delete-transit-gateway` con la `transit-gateway-id`. Para obtener más información sobre `delete-transit-gateway` el comando, consulte delete-transit-gateway.

En el siguiente ejemplo, se elimina `My Transit Gateway`, que se creó en el primer paso anterior:

```
aws ec2 delete-transit-gateway \
  --transit-gateway-id tgw-1234567890abcdef0
```

A continuación, se muestra la respuesta a la solicitud, que incluye el nombre y la ID de la puerta de enlace de tránsito eliminados, junto con las opciones originales definidas para la puerta de enlace de tránsito cuando se creó.

```
{
    "TransitGateway": {
        "TransitGatewayId": "tgw-1234567890abcdef0",
        "TransitGatewayArn": "arn:aws:ec2:us-west-2:123456789012:transit-gateway/
tgw-1234567890abcdef0",
        "State": "deleting",
        "OwnerId": "123456789012",
        "Description": "My Transit Gateway",
        "CreationTime": "2025-06-23T17:39:33+00:00",
        "Options": {
            "AmazonSideAsn": 64512,
            "AutoAcceptSharedAttachments": "disable",
            "DefaultRouteTableAssociation": "enable",
            "AssociationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "DefaultRouteTablePropagation": "enable",
            "PropagationDefaultRouteTableId": "tgw-rtb-abcdef1234567890a",
            "VpnEcmpSupport": "enable",
            "DnsSupport": "enable",
            "SecurityGroupReferencingSupport": "disable",
            "MulticastSupport": "disable"
        },
        "Tags": [
            {
                "Key": "Name",
                "Value": "example-transit-gateway"
            }
        ]
    }
}
```

Conclusión

Creó correctamente una puerta de enlace de tránsito, le conectó dos VPCs , configuró el enrutamiento entre ellas y verificó la conectividad. Este sencillo ejemplo demuestra la funcionalidad básica de las pasarelas de AWS tránsito. Para situaciones más complejas, como conectarse a redes en las instalaciones o implementar configuraciones de enrutamiento más avanzadas, consulte la Guía de AWS Transit Gateways.

Prácticas recomendadas de diseño de AWS Transit Gateway

A continuación, se muestran prácticas recomendadas para el diseño de puerta de enlace de tránsito:

- Utilice una subred independiente para cada archivo asociado a la VPC de la puerta de enlace de tránsito. En cada subred, utilice un CIDR pequeño, por ejemplo `/28`, a fin de tener más direcciones para los recursos de EC2. Cuando utilice una subred independiente, puede configurar los siguientes recursos:
  - Mantenga abierta la ACL de red entrante y saliente asociada con las subredes de puerta de enlace de tránsito.
  - En función del flujo de tráfico, puede aplicar ACL de red a las subredes de carga de trabajo.
- Cree una ACL de red y asóciela con todas las subredes asociadas con la puerta de enlace de tránsito. Mantenga abierta la ACL de red tanto en las direcciones de entrada como de salida.
- Asocie la misma tabla de enrutamiento de VPC con todas las subredes asociadas con la puerta de enlace de tránsito, a no ser que el diseño de red requiera varias tablas de enrutamiento de VPC (por ejemplo, una VPC central que enrute el tráfico a través de varias puertas de enlace NAT).
- Utilice conexiones Site-to-Site VPN de protocolo de puerta de enlace fronteriza (BGP). Si el dispositivo de puerta de enlace de cliente o el firewall de la conexión admite varias rutas, habilite esta característica.
- Habilite la propagación de rutas para las conexiones de puerta de enlace de Direct Connect y las conexiones de BGP de Site-to-Site VPN.
- Cuando migra desde el emparejamiento de VPC para utilizar una puerta de enlace de tránsito. Una discrepancia en el tamaño de la MTU entre el emparejamiento de VPC y la puerta de enlace de tránsito podría provocar la caída de algunos paquetes de tráfico asimétrico. Actualice ambas VPC al mismo tiempo para evitar la caída de paquetes gigantes debido a discrepancias en el tamaño.
- No necesita puerta de enlace de tránsito adicionales para una alta disponibilidad, ya que las puertas de enlace de tránsito cuentan con una disponibilidad elevada por diseño.
- Limite el número de tablas de enrutamiento de puerta de enlace de tránsito a menos que el diseño requiera varias tablas de enrutamiento de puerta de enlace de tránsito.
- Para obtener redundancia, utilice una única puerta de enlace de tránsito en cada región para la recuperación de desastres.

- Para implementaciones con varias puertas de enlace de tránsito, se recomienda que utilice un número de sistema autónomo (ASN) único con cada una de las puertas de enlace de tránsito. También es posible utilizar el emparejamiento entre regiones. Para obtener más información, consulte Creación de una red global mediante el emparejamiento entre regiones de AWS Transit Gateway.

Trabaje con AWS Transit Gateway

Puede usar puerta de enlaces de tránsito mediante la consola de Amazon VPC o la AWS CLI. Para obtener información sobre cómo habilitar y administrar el soporte de cifrado para su pasarela de tránsito, consultethe section called “Encryption Support”.

Temas

puertas de enlace de tránsito compartidas

Puede usar AWS Resource Access Manager (RAM) para compartir una puerta de enlace de tránsito para los archivos adjuntos de la VPC entre cuentas o en toda su organización. AWS Organizations La RAM debe estar habilitada y los recursos deben compartirse con una organización. Para obtener más información, consulte Habilitar el uso compartido de recursos con AWS Organizations en la Guía del usuario de AWS RAM .

Consideraciones

Tenga en cuenta lo siguiente cuando desee compartir una puerta de enlace de tránsito.

- Se debe crear un AWS Site-to-Site VPN archivo adjunto en la misma AWS cuenta propietaria de la pasarela de tránsito.
- Un adjunto a una puerta de enlace de Direct Connect utiliza una asociación de puerta de enlace de tránsito y puede estar en la misma AWS cuenta que la puerta de enlace de Direct Connect o en una cuenta diferente de la puerta de enlace de Direct Connect.

De forma predeterminada, los usuarios no tienen permiso para crear o modificar AWS RAM recursos. Para permitir a los usuarios crear o modificar recursos y realizar tareas, debe crear políticas de IAM que les concedan permisos para usar los recursos y las acciones de la API. A continuación, debe adjuntar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Solo el propietario del recurso puede realizar las siguientes operaciones:

- Crear un recurso compartido
- Actualizar un recurso compartido
- Visualizar un recurso compartido
- Ver los recursos que se comparten a través de su cuenta en todos los recursos compartidos
- Ver las entidades principales con las que comparte sus recursos en todos los recursos compartidos Ver las entidades principales con las que comparte recursos le permite determinar quién tiene acceso a sus recursos compartidos
- Eliminar un recurso compartido
- Ejecute todas las puerta de enlace de tránsito, la puerta de enlaces de tránsito y las API de tablas de enrutamiento de puerta de enlace de tránsito.

Puede realizar las siguientes operaciones en los recursos que han compartido con usted:

- Aceptar o rechazar una invitación para compartir un recurso.
- Visualizar un recurso compartido.
- Ver los recursos compartidos a los que puede acceder.
- Ver una lista de todas las entidades principales que comparten recursos con usted. Ver qué recursos y recursos compartidos han compartido con usted.
- Puede ejecutar la API `DescribeTransitGateways`.
- Ejecutar las API que crean y describen las vinculaciones, por ejemplo: `CreateTransitGatewayVpcAttachment` y `DescribeTransitGatewayVpcAttachments` en sus VPC.

- Abandonar un recurso compartido.

Cuando se comparte una puerta de enlace de tránsito con usted, no puede crear, modificar ni eliminar las tablas de enrutamiento de la puerta de enlace de tránsito, ni las propagaciones y asociaciones de la tabla de enrutamiento de la puerta de enlace de tránsito.

Cuando se crea una puerta de enlace de tránsito, esta se crea en la zona de disponibilidad correspondiente a la cuenta y es independiente de las demás cuentas. Cuando la puerta de enlace de tránsito y las entidades vinculadas están en cuentas diferentes, utilice el ID de zona de disponibilidad para identificar de forma inequívoca y sistemática la zona de disponibilidad. Por ejemplo, use1-az1 es un ID AZ para la región us-east-1 y se asigna a la misma ubicación en todas las cuentas. AWS

Dejar de compartir una puerta de enlace de tránsito

Cuando el propietario del recurso deja de compartir la puerta de enlace de tránsito, se aplican las siguientes reglas:

- La puerta de enlaces de tránsito sigue funcionando.
- La cuenta compartida no puede describir la puerta de enlace de tránsito.
- El propietario de la puerta de enlace de tránsito y el propietario del recurso pueden eliminar la conexión de puerta de enlace de tránsito.

Cuando una pasarela de transporte público deja de compartirse con otra AWS cuenta, o si la AWS cuenta con la que se comparte la pasarela de transporte se elimina de la organización, la propia pasarela de transporte público no se verá afectada.

Subredes compartidas

El propietario de la VPC puede asociar una puerta de enlace de tránsito a una subred de VPC compartida. Los participantes no pueden hacerlo. El tráfico de los recursos del participante puede utilizar los archivos adjuntos en función de las rutas configuradas en la subred de VPC compartida por el propietario de la VPC.

Para obtener más información, consulte Compartir su VPC con otras cuentas en la Guía del usuario de Amazon VPC.

Pasarelas de tránsito en AWS Transit Gateway

Una pasarela de tránsito te permite conectar conexiones VPN VPCs y enrutar el tráfico entre ellas. Una pasarela de transporte funciona de forma transversal y puedes utilizarla AWS RAM para compartirla con otras cuentas. Cuentas de AWS Después de compartir una pasarela de transporte público con otra Cuenta de AWS, el propietario de la cuenta puede adjuntarla VPCs a tu pasarela de transporte público. Un usuario de cualquiera de las cuentas puede eliminar la vinculación en cualquier momento.

Puede habilitar la multidifusión en una puerta de enlace de tránsito y, a continuación, crear un dominio de multidifusión de transit puerta de enlace que permita que el tráfico de multidifusión se envíe desde el origen de multidifusión a los miembros del grupo de multidifusión a través de conexiones de la VPC que asocie con el dominio.

Cada vinculación de VPC o VPN se asocia a una única tabla de enrutamiento. Dicha tabla decide el siguiente salto del tráfico procedente de la vinculación de ese recurso. Una tabla de rutas dentro de la pasarela de transporte IPv4 incluye IPv6 CIDRs ambos destinos. Los objetivos son VPCs las conexiones VPN. Al asociar una VPC o crear una conexión de VPN en una puerta de enlace de tránsito, la conexión se asocia con la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito.

Puede crear tablas de enrutamiento adicionales dentro de la puerta de enlace de tránsito y cambiar la asociación de la VPC o VPN a dichas tablas. Esto le permite segmentar su red. Por ejemplo, puede VPCs asociar el desarrollo a una tabla de rutas y la producción VPCs a una tabla de rutas diferente. Esto le permite crear redes aisladas dentro de una puerta de enlace de tránsito similar al enrutamiento y reenvío virtuales (VRFs) de las redes tradicionales.

Las pasarelas de tránsito admiten el enrutamiento dinámico y estático entre las conexiones conectadas VPCs y las VPN. Puede habilitar o deshabilitar la propagación de rutas para cada vinculación. Los adjuntos de VPN Concentrator solo admiten el enrutamiento BGP (dinámico). Las vinculaciones de interconexión de puerta de enlace solo son compatibles con el enrutamiento estático. Puede dirigir las rutas de las tablas de enrutamiento de la puerta de enlace de tránsito a la vinculación de interconexión para enrutar el tráfico entre las puertas de enlace de tránsito interconectadas.

Si lo desea, puede asociar uno o más bloques IPv4 o bloques IPv6 CIDR a su pasarela de tránsito. Especifique una dirección IP del bloque de CIDR al establecer una interconexión de Transit Gateway Connect para una conexión de Transit Gateway Connect. Puede asociar cualquier rango de direcciones IP públicas o privadas, excepto las direcciones en el rango de

`169.254.0.0/16` y los rangos que se superponen con las direcciones para las vinculaciones de VPC y las redes en las instalaciones. Para obtener más información sobre IPv4 los bloques IPv6 CIDR, consulte el direccionamiento IP en la Guía del usuario de Amazon VPC.

Tareas

- Cree una pasarela de tránsito en AWS Transit Gateway
- Consultar información de la puerta de enlace de tránsito en AWS Transit Gateway
- Administrar etiquetas de la puerta de enlace de tránsito en AWS Transit Gateway
- Modificar una pasarela de tránsito en AWS Transit Gateway
- Acepte un recurso compartido de AWS Transit Gateway mediante la AWS Resource Access Manager consola
- Aceptar una conexión compartida en AWS Transit Gateway
- Eliminar una pasarela de tránsito en AWS Transit Gateway
- Soporte de cifrado para AWS Transit Gateway

Cree una pasarela de tránsito en AWS Transit Gateway

Cuando crea una puerta de enlace de tránsito, se crea una tabla de enrutamiento de la puerta de enlace de tránsito predeterminada y se utiliza como tabla de ruteo de asociación y de propagación predeterminada. Si elige no crear la tabla de enrutamiento de puerta de enlace de tránsito predeterminada, puede crear una más adelante. Para obtener más información acerca de las rutas y las tablas de enrutamiento, consulte ???.

> **Note**
>
> Si quieres habilitar la compatibilidad con el cifrado en una pasarela de tránsito, no puedes habilitarla al crear la pasarela. Una vez que hayas creado la pasarela de tránsito y esté en el estado disponible, podrás modificarla para habilitar la compatibilidad con el cifrado. Para obtener más información, consulte the section called “Encryption Support”.

Para crear una puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways (Puertas de enlace de tránsito).
3. Elija Create Transit Gateway (Crear puerta de enlace de tránsito).

4. En Name tag (Etiqueta de nombre), puede escribir un nombre para la puerta de enlace de tránsito. Una etiqueta de nombre puede facilitar la identificación de una puerta de enlace específica de la lista de puerta de enlaces. Al añadir una Name tag (Etiqueta de nombre), se crea una etiqueta con una clave de Name (Nombre) y el mismo valor que ya ha especificado.
5. En Description (Descripción), puede escribir una descripción para la puerta de enlace de tránsito.
6. En Amazon side Autonomous System Number (ASN) (Número de sistema autónomo (ASN) del lado de Amazon), deje el valor predeterminado, para utilizar el ASN predeterminado, o bien ingrese el ASN privado de la puerta de enlace de tránsito. Debe ser el ASN del AWS lado de una sesión de Border Gateway Protocol (BGP).

   El rango va de 64512 a 65534 para los números de sistema autónomos de 16 bits.

   Para los números de sistema autónomos de 32 bits, el rango va de 4200000000 a 4294967294.

   Si tiene una implementación en varias regiones, recomendamos que utilice un ASN único para cada una de las puerta de enlaces de tránsito.
7. En DNS support (Compatibilidad con DNS), seleccione esta opción si necesita que la VPC resuelva los nombres de host DNS IPv4 públicos en direcciones IPv4 privadas cuando se realicen consultas desde instancias de otra VPC conectada a la puerta de enlace de tránsito.
8. En Compatibilidad de referencia a grupos de seguridad, habilite esta característica para que haga referencia al grupo de seguridad en las VPC conectadas a la puerta de enlace de tránsito. Para obtener más información sobre la referencia a los grupos de seguridad, consulte the section called “Referencia a grupos de seguridad”.
9. En VPN ECMP support (Compatibilidad de ECMP de VPN), seleccione esta opción si necesita compatibilidad de enrutamiento mediante varias rutas de igual costo (ECMP) entre los túneles de la VPN. Si las conexiones anuncian los mismos CIDR, el tráfico se distribuye equitativamente entre ellos.

   Al seleccionar esta opción, el ASN de BGP anunciado y, a continuación, los atributos de BGP, como el, deben ser AS-path los mismos.

   > **Note**
   >
   > Para utilizar ECMP, debe crear una conexión de VPN que utilice enrutamiento dinámico. Las conexiones de VPN que utilizan enrutamiento estático no admiten ECMP.

10. En Default route table association (Asociación de tabla de enrutamiento predeterminada), seleccione esta opción para asociar automáticamente las conexiones de puerta de enlace de tránsito a la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito.
11. En Default route table propagation (Propagación de tabla de enrutamiento predeterminada), seleccione esta opción para propagar automáticamente las conexiones de puerta de enlace de tránsito a la tabla de enrutamiento predeterminada de la puerta de enlace de tránsito.
12. (Opcional) Para utilizar la puerta de enlace de tránsito como enrutador para el tráfico de multidifusión, seleccione Multicast support (Compatibilidad con la multidifusión).
13. (Opcional) En la sección de opciones Configure-cross-account para compartir, selecciona si deseas aceptar automáticamente los archivos adjuntos compartidos. Si la opción está habilitada, las conexiones se aceptan automáticamente. De lo contrario, debe aceptar o rechazar las solicitudes de conexión.

    En Auto accept shared attachments (Aceptar conexiones compartidas automáticamente), seleccione esta opción para aceptar automáticamente las conexiones entre cuentas.
14. (Opcional) en Transit puerta de enlace CIDR blocks (Bloques de CIDR de la puerta de enlace de tránsito), especifique uno o varios bloques de CIDR IPv4 o IPv6 para la puerta de enlace de tránsito.

    Puede especificar un bloque de CIDR de tamaño /24 o mayor (por ejemplo, /23 o /22) para IPv4, o un bloque de CIDR de tamaño /64 o mayor (por ejemplo, /63 o /62) para IPv6. Puede asociar cualquier rango de direcciones IP públicas o privadas, excepto las direcciones de la 169.254.0.0/16 rango y rangos que se superponen con las direcciones de los adjuntos de la VPC y las redes locales.

    > **Note**
    >
    > Los bloques CIDR de Transit Gateway se utilizan si está configurando archivos adjuntos de Connect (GRE), VPN de IP privada o archivos adjuntos de VPN de cliente. Transit Gateway asigna direcciones IP a los puntos finales del túnel (GRE/PrivateIP VPN) y a los adjuntos de Client VPN de este rango.
15. Elija Create Transit Gateway (Crear puerta de enlace de tránsito).

Para crear una pasarela de tránsito mediante el AWS CLI

Utilice el comando create-transit-gateway.

Consultar información de la puerta de enlace de tránsito en AWS Transit Gateway

Consulte todas sus puertas de enlace de tránsito.

Para consultar una puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways (Puertas de enlace de tránsito). Los detalles de la puerta de enlace de tránsito se muestran debajo de la lista de puertas de enlaces en la página.

Para consultar una puerta de enlace de tránsito con la AWS CLI

Utilice el comando describe-transit-gateways.

Administrar etiquetas de la puerta de enlace de tránsito en AWS Transit Gateway

Añada etiquetas a sus recursos para organizarlos e identificarlos mejor, por ejemplo, por objetivo, propietario o entorno. Puede agregar varias etiquetas a cada puerta de enlace de tránsito. Las claves de etiqueta deben ser únicas para cada puerta de enlace de tránsito. Si agrega una etiqueta con una clave que ya está asociada a la puerta de enlace de tránsito, se actualiza el valor de esa etiqueta. Para obtener más información, consulte Etiquetado de los recursos de Amazon EC2.

Agregar etiquetas a una puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways (Puertas de enlace de tránsito).
3. Seleccione la puerta de enlace de tránsito a la que quiere agregar etiquetas o cuyas etiquetas desea editar.
4. Elija la pestaña Tags (Etiquetas) en la parte inferior de la página.
5. Elija Manage tags (Administrar etiquetas).
6. Elija Add new tag (Agregar nueva etiqueta).
7. Escriba una Key (Clave) y un Value (Valor) para la etiqueta.
8. Seleccione Save.

Modificar una pasarela de tránsito en AWS Transit Gateway

Puede modificar las opciones de configuración para una puerta de enlace de tránsito. Al modificar una puerta de enlace de tránsito, las conexiones de la puerta de enlace de tránsito existentes no sufren ninguna interrupción del servicio.

No puede modificar una puerta de enlace de tránsito que se haya compartido con usted.

No puede eliminar un bloque de CIDR para la gateway de tránsito si alguna de las direcciones IP se utiliza actualmente para una interconexión de Connect.

> **Note**
>
> Las pasarelas de tránsito que tienen habilitado el soporte de cifrado se pueden conectar VPCs con los controles de cifrado en modo monitor o cumplimiento, o VPCs que no tienen los controles de cifrado habilitados. VPCs que tienen controles de cifrado en modo Enforce SOLO se pueden conectar a Transit Gateways que tengan habilitado el soporte de cifrado. Para obtener información más detallada, consulte the section called “Encryption Support”.

Para modificar una puerta de enlace de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways (Gateways de tránsito).
3. Elija la puerta de enlace de tránsito que desea modificar.
4. Elija Actions (Acciones), Modify transit puerta de enlace (Modificar puerta de enlace de tránsito).
5. Modifique las opciones según sea necesario y elija Modify transit puerta de enlace (Modificar puerta de enlace de tránsito).

Para modificar su pasarela de tránsito mediante el AWS CLI

Utilice el comando modify-transit-gateway.

Acepte un recurso compartido de AWS Transit Gateway mediante la AWS Resource Access Manager consola

Si le han añadido a un recurso compartido, recibirá una invitación para unirse a este. Para poder obtener acceso a los recursos compartidos, antes se debe aceptar el uso compartido del recurso mediante la consola AWS Resource Access Manager (AWS RAM).

Para aceptar el uso compartido de un recurso

1. Abre la AWS RAM consola en https://console.aws.amazon.com/ram/.
2. En el panel de navegación, elija Shared with me (Compartidos conmigo), Resource shares (Recursos compartidos).
3. Seleccione el recurso compartido.
4. Elija Accept resource share (Aceptar el uso compartido de recursos).
5. Para consultar la puerta de enlace de tránsito compartida, abra la página Transit Gateways (Puertas de enlace de tránsito) en la consola de Amazon VPC.

Aceptar una conexión compartida en AWS Transit Gateway

Si no habilitó la función Aceptación automática de conexiones compartidas al crear la puerta de enlace de tránsito, debe aceptar manualmente las conexiones entre cuentas (compartidas) ya sea desde la consola de Amazon VPC o la CLI de AWS.

Para aceptar manualmente una vinculación

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Conexiones de puerta de enlace de tránsito).
3. Seleccione la conexión de puerta de enlace de tránsito pendiente de aceptación.
4. Elija Actions (Acciones), Accept transit gateway attachment (Aceptar conexión de puerta de enlace de tránsito).

Para aceptar una vinculación compartida mediante la AWS CLI

Utilice el comando accept-transit-gateway-vpc-attachment.

Eliminar una pasarela de tránsito en AWS Transit Gateway

No puede eliminar una puerta de enlace de tránsito con conexiones existentes. Para poder eliminar una puerta de enlace de tránsito antes debe eliminar todas las conexiones.

Para eliminar una puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. Elija la puerta de enlace de tránsito que desea eliminar.
3. Elija Actions (Acciones), Delete transit gateway (Eliminar puerta de enlace de tránsito). Ingrese **`delete`** y elija Delete (Eliminar) para confirmar la eliminación.

Para eliminar una pasarela de tránsito mediante el AWS CLI

Utilice el comando delete-transit-gateway.

Soporte de cifrado para AWS Transit Gateway

Los controles de cifrado le permiten auditar el estado de cifrado de los flujos de tráfico de la VPC y, a continuación, aplicar el cifrado en tránsito para todo el tráfico de la VPC. Cuando el control de cifrado de la VPC esté en modo obligatorio, todas las interfaces de red elásticas (ENI) de esa VPC estarán restringidas para conectarse únicamente a instancias con capacidad de cifrado de AWS Nitro; y solo los AWS servicios que cifran datos en tránsito podrán conectarse a la VPC forzada por Encryption Controls. Para obtener más información sobre los controles de cifrado de VPC, consulte esta documentación.

Transit Gateway Encryption Support y control de cifrado de VPC

El soporte de cifrado de Transit Gateway le permite aplicar el cifrado en tránsito para el tráfico entre las VPC conectadas a una Transit Gateway. Deberá activar manualmente Encryption Support en Transit Gateway mediante el comando modify-transit-gateway para cifrar el tráfico entre las VPC. Una vez activado, todo el tráfico atravesará los enlaces cifrados al 100% entre las VPC que estén en modo Enforce (sin exclusiones) a través de Transit Gateway. También puede conectar VPC que no tengan los controles de cifrado activados o que estén en modo Monitor a través de una Transit Gateway que tenga activado Encryption Support. En este escenario, se garantiza que Transit Gateway cifra el tráfico hasta el adjunto de Transit Gateway en la VPC que no se ejecuta en modo obligatorio. Más allá de eso, depende de la instancia a la que se envía el tráfico en la VPC que no se ejecuta en modo de aplicación.

Solo puedes añadir soporte de cifrado a una pasarela de tránsito existente y no mientras estás creando una. A medida que la Transit Gateway pase al estado Encryption Support Enabled, no habrá tiempo de inactividad en la Transit Gateway ni en los archivos adjuntos. La migración es fluida y transparente, sin que se interrumpa el tráfico. Para conocer los pasos para modificar una pasarela de tránsito para añadir Encryption Support, consulteModificar un puerta de enlace de tránsito.

Requisitos

Antes de habilitar la compatibilidad con el cifrado en una pasarela de tránsito, asegúrese de que:

- La pasarela de transporte público no tiene archivos adjuntos de Connect
- La pasarela de transporte público no tiene archivos adjuntos de interconexión
- La puerta de enlace de tránsito no tiene adjuntos de Network Firewall
- La puerta de enlace de tránsito no tiene archivos adjuntos a un concentrador VPN
- La pasarela de tránsito no tiene adjuntos de Client VPN
- La pasarela de tránsito no tiene habilitadas las referencias a grupos de seguridad
- La pasarela de tránsito no tiene habilitadas las funciones de multidifusión

Estados de Encryption Support

Una pasarela de tránsito puede tener uno de los siguientes estados de cifrado:

- activación: la puerta de enlace de tránsito está habilitando el soporte de cifrado. Este proceso puede tardar hasta 14 días en completarse.
- activado: la compatibilidad con el cifrado está habilitada en la pasarela de tránsito. Puede crear adjuntos de VPC con el control de cifrado aplicado.
- inhabilitación: la pasarela de tránsito está inhabilitando la compatibilidad con el cifrado.
- deshabilitado: el soporte de cifrado está deshabilitado en la pasarela de tránsito.

Reglas de anclaje de Transit Gateway

Cuando una pasarela de tránsito tiene habilitada la compatibilidad con el cifrado, se aplican las siguientes reglas de adjuntos:

- Cuando el estado de cifrado de la puerta de enlace de tránsito esté activado o desactivado, puede crear adjuntos de Direct Connect, adjuntos de VPN y adjuntos de VPC que no estén en el modo obligatorio o obligatorio del Control de cifrado.

- Cuando el estado de cifrado de la puerta de enlace de tránsito está habilitado, puede crear archivos adjuntos de VPC, archivos adjuntos de Direct Connect, archivos adjuntos de VPN y archivos adjuntos de VPC en cualquier modo de control de cifrado.
- Cuando el estado de cifrado de la puerta de enlace de tránsito está deshabilitado, no puede crear nuevos adjuntos de VPC con el control de cifrado impuesto.
- Encryption Support no admite los adjuntos de Connect, los adjuntos de Peering, los adjuntos de Network Firewall, los adjuntos de VPN Concentrator, los adjuntos de Client VPN, las referencias a grupos de seguridad y las funciones de multidifusión.

Si se intenta crear archivos adjuntos incompatibles, se producirá un error en la API.

Archivos adjuntos de Amazon VPC en AWS Transit Gateway

Un adjunto Amazon Virtual Private Cloud (VPC) a una puerta de enlace de tránsito le permite enrutar el tráfico hacia y desde una o más subredes de VPC. Cuando asocia una VPC a una puerta de enlace de tránsito, debe especificar una subred de cada zona de disponibilidad que la puerta de enlace de tránsito utilizará para enrutar el tráfico. Las subredes especificadas sirven como puntos de entrada y salida para el tráfico de la puerta de enlace de tránsito. El tráfico solo puede llegar a los recursos de otras subredes dentro de la misma zona de disponibilidad si las subredes de conexión de puerta de enlace de tránsito tienen las rutas adecuadas configuradas en sus tablas de enrutamiento que apuntan a las subredes de destino.

Límites

- Cuando se asocia una VPC a una puerta de enlace de tránsito, los recursos en zonas de disponibilidad donde no hay una conexión de puerta de enlace de tránsito no pueden llegar a la puerta de enlace de tránsito.

> **Note**
>
> Dentro de las zonas de disponibilidad que sí tienen conexiones de puerta de enlace de tránsito, el tráfico solo se reenvía a la puerta de enlace de tránsito desde las subredes específicas que están asociadas a la conexión. Si hay una ruta a la puerta de enlace de tránsito en una tabla de enrutamiento de subred, el tráfico solo se reenvía a la puerta de enlace de tránsito cuando esta tenga una conexión en una subred en la misma zona de

disponibilidad y la tabla de enrutamiento de la subred contiene rutas apropiadas para el destino previsto del tránsito dentro de la VPC.

- Una puerta de enlace de tránsito no admite la resolución de DNS para los nombres DNS personalizados de la VPCs configuración adjunta mediante zonas alojadas privadas en Amazon Route 53. Para configurar la resolución de nombres para las zonas alojadas privadas para todas las VPCs conectadas a una puerta de enlace de tránsito, consulte Administración centralizada de DNS de la nube híbrida con Amazon Route 53 y AWS Transit Gateway.
- Una puerta de enlace de tránsito no admite el enrutamiento entre VPCs una CIDRs VPC conectada o si una CIDR de un rango se superpone a una CIDR de una VPC conectada. Si se conecta una VPC a una puerta de enlace de tránsito y su CIDR es idéntico a, o se superpone con, el CIDR de otra VPC que ya esté conectada a la puerta de enlace de tránsito, las rutas de la VPC recientemente conectada no se propagan a la tabla de enrutamiento de la puerta de enlace de tránsito.
- No puede crear una asociación para una subred de VPC que resida en una zona local. Sin embargo, puede configurar la red para que las subredes de la zona local se puedan conectar a una puerta de enlace de tránsito mediante la zona de disponibilidad principal. Para obtener más información, consulte Conexión de las subredes de una zona local a una puerta de enlace de tránsito.
- No puedes crear un adjunto a una pasarela de tránsito utilizando subredes exclusivas. IPv6 Las subredes adjuntas a las pasarelas de tránsito también deben admitir direcciones. IPv4
- Una puerta de enlace de tránsito debe tener al menos una conexión de VPC antes de poder agregar esa puerta de enlace de tránsito a una tabla de enrutamiento.

Requisitos de la tabla de enrutamiento para conexiones de VPC

Las conexiones de VPC de la puerta de enlace de tránsito requieren configuraciones de tabla de enrutamiento específicas para funcionar correctamente:

- Tablas de enrutamiento de subred vinculadas: las subredes asociadas a la conexión de puerta de enlace de tránsito deben tener entradas en la tabla de enrutamiento para cualquier destino en la VPC al que se deba acceder a través de la puerta de enlace de tránsito. Esto incluye rutas a otras subredes, puertas de enlace de Internet, puertas de enlace NAT y puntos de conexión de VPC.
- Tablas de enrutamiento de las subredes de destino: las subredes que contienen recursos que deben comunicarse a través de la puerta de enlace de tránsito deben tener rutas que apunten hacia la puerta de enlace de tránsito para el tráfico de retorno a destinos externos.

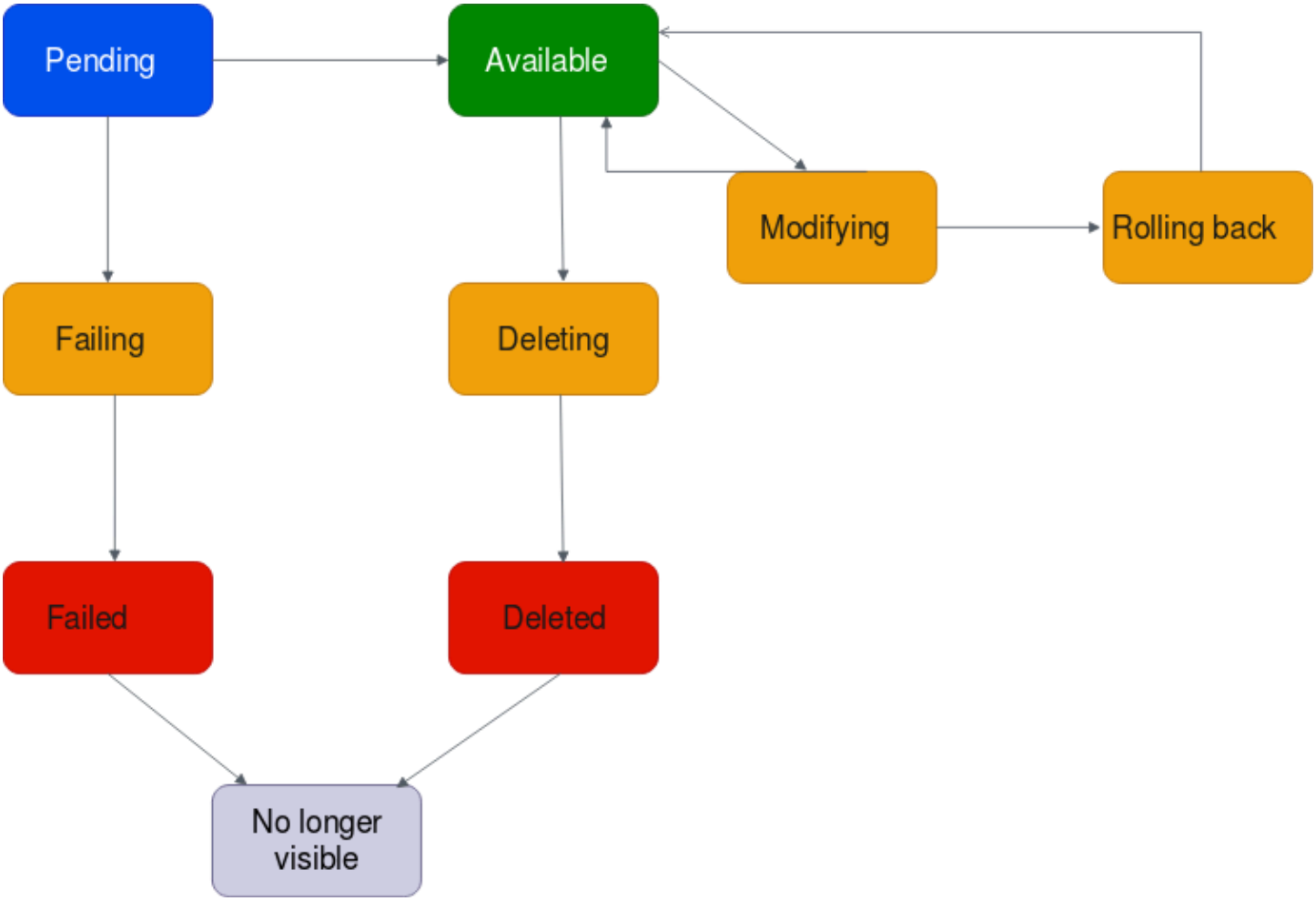
- Tráfico de VPC local: la conexión de puerta de enlace de tránsito no habilita automáticamente la comunicación entre subredes de la misma VPC. Se aplican las reglas de enrutamiento de VPC estándar y la ruta local (CIDR de VPC) debe estar presente en las tablas de enrutamiento para la comunicación dentro de la VPC.

> **Note**
>
> Tener rutas configuradas en subredes no conectadas dentro de la misma zona de disponibilidad no permite el flujo de tráfico. Solo las subredes específicas asociadas al adjunto a la puerta de enlace de tránsito pueden servir como entry/exit puntos para el tráfico de la puerta de enlace de tránsito.

Ciclo de vida de la conexión de VPC

Una conexión de VPC pasa por varias etapas, desde que se inicia la solicitud. En cada una de estas fases, se encontrará con acciones que podrá realizar y, al final del ciclo de vida, la conexión de la VPC permanecerá visible en la Amazon Virtual Private Cloud Console y en la API o los resultados de la línea de comandos durante un tiempo.

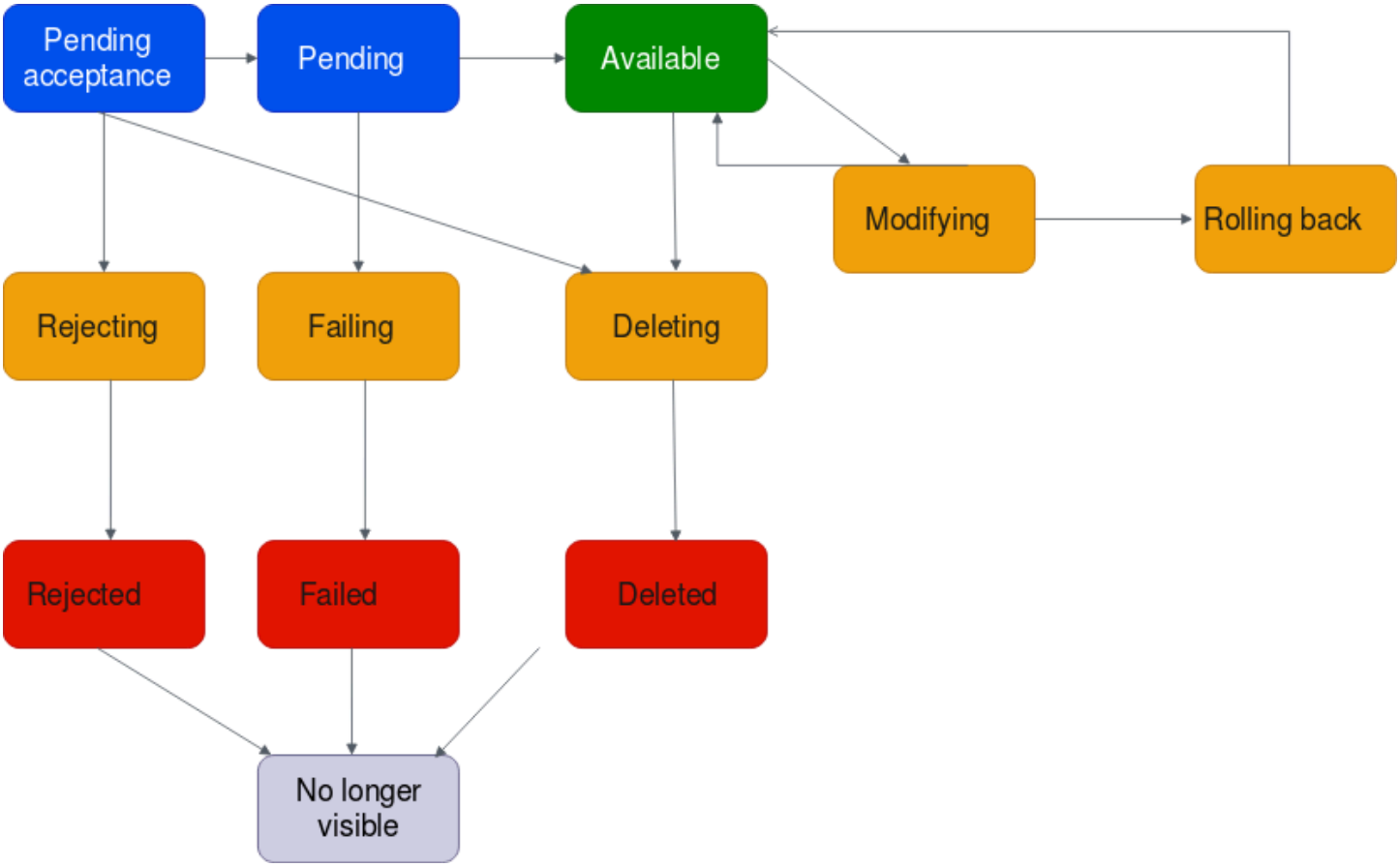
El siguiente diagrama muestra los estados por los que puede pasar una conexión en una única configuración de cuenta, o una configuración entre cuentas que tenga activada la opción Aceptar automáticamente las conexiones compartidas .



- Pendiente: se inició una solicitud para una conexión de VPC y está en proceso de aprovisionamiento. En esta etapa, es posible que se produzca un error en la conexión o puede ir a `available`.
- Errónea: se ha producido un error en una solicitud de conexión de VPC. En esta etapa, la conexión de VPC va a `failed`.
- Con error: se ha producido un error en la solicitud de conexión de VPC. Mientras se encuentre en este estado, no se puede eliminar. La conexión de VPC que produjo errores permanece visible durante 2 horas y, luego, ya no estará visible.
- Disponible: la conexión de VPC está disponible y el tráfico puede fluir entre la VPC y la puerta de enlace de tránsito. En esta etapa, la conexión puede ir a `modifying` o a `deleting`.
- Eliminando: una conexión de VPC que se está en proceso de ser eliminada. En esta etapa, la conexión puede ir a `deleted`.

- Eliminada: se eliminó una conexión de VPC de `available`. Mientras se encuentre en este estado, la conexión de VPC no se puede modificar. La conexión de VPC permanece visible durante 2 horas y, luego, ya no estará visible.
- Modificando: se realizó una solicitud para modificar las propiedades de la conexión de VPC. En esta etapa, la conexión puede ir a `available` o a `rolling back`.
- Reversión: no se puede completar la solicitud de modificación de la conexión de VPC y el sistema está deshaciendo los cambios realizados. En esta etapa, la conexión puede ir a `available`.

El siguiente diagrama muestra los estados por los que puede pasar una conexión en una configuración entre cuentas que tenga desactivada la opción Auto accept shared attachments (Aceptar automáticamente las conexiones compartidas).



- Aceptación pendiente: la solicitud de conexión de VPC está esperando la aceptación. En esta etapa, la conexión puede ir a `pending`, a `rejecting` o a `deleting`.
- Rechazando: una conexión de VPC que está en proceso de ser rechazada. En esta etapa, la conexión puede ir a `rejected`.

- Rechazado: se rechazó una conexión de VPC de `pending acceptance`. Mientras se encuentre en este estado, la conexión de VPC no se puede modificar. La conexión de VPC permanece visible durante 2 horas y, luego, ya no estará visible.
- Pendiente: se aceptó la conexión de VPC y está en proceso de aprovisionamiento. En esta etapa, es posible que se produzca un error en la conexión o puede ir a `available`.
- Errónea: se ha producido un error en una solicitud de conexión de VPC. En esta etapa, la conexión de VPC va a `failed`.
- Con error: se ha producido un error en la solicitud de conexión de VPC. Mientras se encuentre en este estado, no se puede eliminar. La conexión de VPC que produjo errores permanece visible durante 2 horas y, luego, ya no estará visible.
- Disponible: la conexión de VPC está disponible y el tráfico puede fluir entre la VPC y la puerta de enlace de tránsito. En esta etapa, la conexión puede ir a `modifying` o a `deleting`.
- Eliminando: una conexión de VPC que se está en proceso de ser eliminada. En esta etapa, la conexión puede ir a `deleted`.
- Eliminada: se eliminó una conexión de VPC de `available` o `pending acceptance`. Mientras se encuentre en este estado, la conexión de VPC no se puede modificar. La conexión de VPC permanece visible durante 2 horas y, luego, ya no estará visible.
- Modificando: se realizó una solicitud para modificar las propiedades de la conexión de VPC. En esta etapa, la conexión puede ir a `available` o a `rolling back`.
- Reversión: no se puede completar la solicitud de modificación de la conexión de VPC y el sistema está deshaciendo los cambios realizados. En esta etapa, la conexión puede ir a `available`.

Modo Dispositivo

Si piensa configurar un dispositivo de red con estado en la VPC, puede habilitar la compatibilidad en modo dispositivo para la conexión de VPC en la que se encuentra el dispositivo cuando crea una conexión. Esto garantiza que AWS Transit Gateway utilice la misma zona de disponibilidad para ese adjunto de VPC durante toda la vida útil del flujo de tráfico entre un origen y un destino. También permite que una puerta de enlace de tránsito envíe tráfico a cualquier zona de disponibilidad de la VPC, siempre y cuando exista una asociación de subred en esa zona. Si bien el modo dispositivo solo se admite en las conexiones de VPC, el flujo de red puede provenir de cualquier otro tipo de conexión de puerta de enlace de tránsito, incluidas conexiones de VPC, VPN y Connect. El modo dispositivo también funciona para flujos de red que tienen orígenes y destinos en diferentes Regiones de AWS. Es posible que los flujos de red se reequilibren entre distintas zonas de disponibilidad si no

se habilita inicialmente el modo dispositivo, sino que se modifica posteriormente la configuración de las conexiones para habilitarlo. Puede utilizar la consola, la línea de comando o la API para habilitar o deshabilitar el modo de dispositivo.

El modo dispositivo de AWS Transit Gateway optimiza el enrutamiento del tráfico teniendo en cuenta las zonas de disponibilidad de origen y destino al determinar la ruta a través de una VPC en modo dispositivo. Este enfoque mejora la eficiencia y reduce la latencia. El comportamiento varía en función de la configuración específica y los patrones de tráfico. A continuación, se presentan algunos ejemplos.

Ejemplo 1: Enrutamiento del tráfico de la zona de disponibilidad mediante la VPC del dispositivo

Cuando el tráfico fluye desde la zona de disponibilidad de origen us-east-1a a la zona de disponibilidad de destino us-east-1a, con conexiones de VPC en modo de dispositivo tanto en us-east-1a como en us-east-1b, la puerta de enlace de tránsito selecciona una interfaz de red de us-east-1a dentro de la VPC del dispositivo. Esta zona de disponibilidad se mantiene durante todo el flujo de tráfico entre el origen y el destino.

Ejemplo 2: Enrutamiento del tráfico dentro de la zona de disponibilidad mediante la VPC del dispositivo

En el caso del tráfico que fluye desde la zona de disponibilidad de origen us-east-1a a la zona de disponibilidad de destino us-east-1b, con conexiones de VPC en modo de dispositivo tanto en us-east-1a como en us-east-1b, la puerta de enlace de tránsito utiliza un algoritmo de hash de flujo para seleccionar us-east-1a o us-east-1b dentro de la VPC del dispositivo. La zona de disponibilidad elegida se utiliza de forma coherente durante todo el flujo.

Ejemplo 3: Enrutamiento del tráfico a través de una VPC de dispositivo sin datos de zona de disponibilidad

Cuando el tráfico se origina en la zona de disponibilidad de origen us-east-1a a un destino sin información de la zona de disponibilidad (p. ej., tráfico destinado a Internet), con conexiones de VPC en modo de dispositivo tanto en us-east-1a como en us-east-1b, la puerta de enlace de tránsito selecciona una interfaz de red de us-east-1a dentro de la VPC del dispositivo.

Ejemplo 4: Enrutamiento del tráfico a través de la VPC de un dispositivo en una zona de disponibilidad distinta de la de origen o de destino

Cuando el tráfico fluye desde la zona de disponibilidad de origen us-east-1a a la zona de disponibilidad de destino us-east-1b, con conexiones de VPC en modo de dispositivo en diferentes zonas de disponibilidad, por ejemplo, en us-east-1c y us-east-1d, la puerta de enlace de tránsito selecciona un algoritmo de hash de flujo para seleccionar us-east-1c o us-east-1d en la VPC del dispositivo. La zona de disponibilidad elegida se utiliza de forma coherente durante todo el flujo.

> **Note**
>
> El modo dispositivo solo se admite para las conexiones de VPC. Asegúrese de que la propagación de rutas esté habilitada para una tabla de enrutamiento asociada a una conexión de VPC del dispositivo.

Referencia a grupos de seguridad

Puede utilizar esta función para simplificar la administración de los grupos de seguridad y el control del instance-to-instance tráfico entre los VPCs que están conectados a la misma puerta de enlace de tránsito. Solo puede hacer referencia cruzada a los grupos de seguridad en las reglas entrantes. Las reglas de seguridad salientes no son compatibles con las referencias a los grupos de seguridad. El uso y la habilitación de las referencias a los grupos de seguridad no tienen costos adicionales.

La compatibilidad con las referencias a los grupos de seguridad se puede configurar tanto para las puertas de enlace de tránsito como para las conexiones de VPC de las puertas de enlace de tránsito, y solo funcionará si se habilitó tanto para una puerta de enlace de tránsito como para sus conexiones de VPC.

Limitaciones

Las siguientes limitaciones se aplican cuando se usa la referencia a los grupos de seguridad con conexiones de VPC.

- No se admite la referencia a grupos de seguridad en las conexiones de interconexión de la puerta de enlace de tránsito. Ambas VPCs deben estar conectadas a la misma pasarela de tránsito.
- La referencia a los grupos de seguridad no es compatible con las conexiones de VPC en la zona de disponibilidad use1-az3.

- No se admite la referencia a grupos de seguridad en los puntos PrivateLink finales. Como alternativa, recomendamos utilizar reglas de seguridad de IP basadas en el CIDR.
- La referencia a los grupos de seguridad funciona para Elastic File System (EFS) siempre que se haya configurado una regla de grupo de seguridad que permita todas las salidas para las interfaces de EFS de la VPC.
- La conectividad de zona local a través de una puerta de enlace de tránsito solo es compatible con las siguientes zonas locales: us-east-1-atl-2a, us-east-1-dfw-2a, us-east-1-iah-2a, us-west-2-lax-1a, us-west-2-lax-1b, us-east-1-mia-2a, us-east-1-chi-2a y us-west-2-phx-2a.
- Recomendamos deshabilitar esta función en el nivel VPCs de conexión de la VPC si las subredes se encuentran en Zonas Locales AWS , Outposts y Wavelength Zones no compatibles AWS , ya que podría provocar una interrupción del servicio.
- Si tiene una VPC de inspección, la referencia a grupos de seguridad a través de la puerta de enlace de tránsito no funciona en el Gateway Load AWS Balancer o en un Network Firewall. AWS

Tareas

- Crear una vinculación de de VPC en AWS Transit Gateway
- Modificar un adjunto de VPC en AWS Transit Gateway
- Modificación de las etiquetas de vinculaciones de la VPC en AWS Transit Gateway
- Consultar una conexión de VPC en AWS Transit Gateway
- Eliminar una conexión de VPC en AWS Transit Gateway
- Actualización de las reglas de entrada del grupo de seguridad de AWS Transit Gateway
- Identificación de los grupos de seguridad referenciados de AWS Transit Gateway
- Eliminación de las reglas obsoletas del grupo de seguridad de AWS Transit Gateway
- Solución de problemas con la creación de conexiones de VPC en AWS Transit Gateway

Crear una vinculación de de VPC en AWS Transit Gateway

Para crear una vinculación de VPC con la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).

3. Elija Create transit puerta de enlace attachment (Crear conexión de puerta de enlace de tránsito).
4. En Name tag (Etiqueta de nombre), opcionalmente puede ingresar un nombre para la conexión de puerta de enlace de tránsito.
5. En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito para la conexión. Puede elegir una puerta de enlace de tránsito de su propiedad o una puerta de enlace de tránsito que se compartió con usted.
6. En Attachment type (Tipo de vinculación), elija VPC.
7. Seleccione si desea habilitar Compatibilidad de DNS, Compatibilidad de IPv6 y Compatibilidad del modo dispositivo.

   Si selecciona el modo dispositivo, el flujo de tráfico entre un origen y un destino utiliza la misma zona de disponibilidad para la conexión de VPC durante la vida útil del flujo.
8. Seleccione si desea habilitar Compatibilidad de referencia a grupos de seguridad. Habilite esta característica para que haga referencia al grupo de seguridad en las VPC conectadas a la puerta de enlace de tránsito. Para obtener más información sobre la referencia a los grupos de seguridad, consulte the section called “Referencia a grupos de seguridad”.
9. Seleccione si desea habilitar Compatibilidad de IPv6.
10. En VPC ID (ID de VPC), elija la VPC que desee asociar a la puerta de enlace de tránsito.

    Esta VPC debe tener una subred asociada como mínimo.
11. En Subnet IDs (ID de subred), seleccione una subred para cada zona de disponibilidad que la puerta de enlace de tránsito utilizará para enrutar el tráfico. Debe seleccionar al menos una subred. Solo puede seleccionar una subred por zona de disponibilidad.
12. Elija Create transit puerta de enlace attachment (Crear conexión de puerta de enlace de tránsito).

Para crear una vinculación de VPC con la AWS CLI

Utilice el comando create-transit-gateway-vpc-attachment.

Modificar un adjunto de VPC en AWS Transit Gateway

Para modificar las vinculaciones de VPC mediante la consola

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

2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la conexión de VPC, y luego elija Actions (Acciones), Modify transit puerta de enlace attachment (Modificar conexión de puerta de enlace de tránsito).
4. Habilite o deshabilite cualquiera de las siguientes opciones:
   - Compatibilidad con DNS
   - IPv6 soporte
   - Compatibilidad del modo dispositivo
5. Para agregar o eliminar una subred de la conexión, marque o desmarque la casilla de verificación ubicada junto a la ID de subred que desea agregar o eliminar.

   > **Note**
   >
   > Agregar o modificar una subred de datos adjuntos de VPC podría afectar el tráfico de datos mientras el adjunto se encuentra en estado de modificación.

6. Para poder hacer referencia a un grupo de seguridad VPCs conectado a una puerta de enlace de tránsito, seleccione el soporte de referencia de grupos de seguridad. Para obtener más información sobre la referencia a los grupos de seguridad, consulte the section called “Referencia a grupos de seguridad”.

   > **Note**
   >
   > Si deshabilita la referencia a los grupos de seguridad para una puerta de enlace de tránsito existente, se deshabilitará en todas las conexiones de la VPC.

7. Elija Modify transit puerta de enlace attachment (Modificar conexión de puerta de enlace de tránsito).

Para modificar los adjuntos de la VPC mediante el AWS CLI

Utilice el comando modify-transit-gateway-vpc-attachment.

Modificación de las etiquetas de vinculaciones de la VPC en AWS Transit Gateway

Para modificar las etiquetas de vinculaciones de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la conexión de VPC, y luego elija Actions (Acciones), Manage tags (Administrar etiquetas).
4. [Agregar una etiqueta] Elija Add new tag (Agregar etiqueta) y haga lo siguiente:
   - En Clave, escriba el nombre de la clave.
   - En Value (Valor), escriba el valor de la clave.
5. [Eliminar una etiqueta] Junto a la etiqueta, elija Remove (Quitar).
6. Seleccione Save.

Las etiquetas de adjunto de VPC solo se pueden modificar con la consola.

Consultar una conexión de VPC en AWS Transit Gateway

Para ver las vinculaciones de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. En la columna Resource type (Tipo de recurso), busque VPC (VPC). Se trata de las conexiones de VPC.
4. Seleccione una vinculación para ver sus detalles.

Para ver las vinculaciones de VPC mediante la AWS CLI

Utilice el comando describe-transit-gateway-vpc-attachments.

Eliminar una conexión de VPC en AWS Transit Gateway

Para eliminar una vinculación de VPC mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la vinculación de VPC.
4. Elija Actions (Acciones),Delete transit gateway attachment (Eliminar conexión de puerta de enlace de tránsito).
5. Cuando se le solicite, ingrese **`delete`** y elija Delete (Eliminar).

Para eliminar una vinculación de VPC mediante la AWS CLI

Utilice el comando delete-transit-gateway-vpc-attachment.

Actualización de las reglas de entrada del grupo de seguridad de AWS Transit Gateway

Puede actualizar todas las reglas de entrada del grupo de seguridad asociadas con la puerta de enlace de tránsito. Para actualizar las reglas del grupo de seguridad desde la consola de Amazon VPC o con la línea de comando o una API. Para obtener más información sobre la referencia a los grupos de seguridad, consulte the section called “Referencia a grupos de seguridad”.

Para actualizar las reglas del grupo de seguridad desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Grupos de seguridad.
3. Para modificar las reglas de entrada, seleccione el grupo de seguridad y luego elija Acciones, Editar reglas de entrada.
4. Para agregar una regla, elija Agregar regla y especifique el tipo, el protocolo y el rango de puertos. En Origen (regla de entrada), ingrese el ID del grupo de seguridad de la VPC conectado a la puerta de enlace de tránsito.

> **Note**
>
> Los grupos de seguridad de una VPC conectados a la puerta de enlace de tránsito no se muestran automáticamente.

5. Para editar una regla existente, cambie los valores (por ejemplo, el origen o la descripción).
6. Para eliminar una regla, elija la opción Eliminar situada junto a la regla.
7. Seleccione Guardar reglas.

Para actualizar las reglas de entrada mediante la línea de comandos

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)
- revoke-security-group-ingress (AWS CLI)

Identificación de los grupos de seguridad referenciados de AWS Transit Gateway

Para determinar si se hace referencia a su grupo de seguridad en las reglas de un grupo de seguridad de una VPC conectada a la misma puerta de enlace de tránsito, utilice uno de los siguientes comandos.

- describe-security-group-references (AWS CLI)
- Get-EC2SecurityGroupReference (AWS Tools for Windows PowerShell)

Eliminación de las reglas obsoletas del grupo de seguridad de AWS Transit Gateway

Una regla obsoleta del grupo de seguridad es una regla que hace referencia a un grupo de seguridad eliminado en la misma VPC o en una VPC conectada a la misma puerta de enlace de tránsito. Cuando una regla de grupo de seguridad queda obsoleta, esta no se quita automáticamente del grupo de seguridad, sino que debe quitarla manualmente.

Puede consultar y eliminar las reglas de grupo de seguridad obsoletas de una VPC mediante la consola de Amazon VPC.

Para ver y eliminar reglas de grupo de seguridad obsoletas

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Security groups (Grupos de seguridad).
3. Elija Actions (Acciones), Manage stale rules (Administrar reglas obsoletas).
4. En VPC, elija la VPC con las reglas obsoletas.
5. Elija Edit.
6. Presione el botón Delete (Eliminar), que se encuentra junto a la regla que desea eliminar. Elija Vista previa de cambios, Guardar reglas.

Descripción de las reglas de grupo de seguridad obsoletas mediante la línea de comandos

- describe-stale-security-groups (AWS CLI)
- Get-EC2StaleSecurityGroup (AWS Tools for Windows PowerShell)

Una vez identificadas las reglas de grupo de seguridad obsoletas, puede eliminarlas utilizando los comandos revoke-security-group-ingress o revoke-security-group-egress.

Solución de problemas con la creación de conexiones de VPC en AWS Transit Gateway

El siguiente tema le puede ayudar a solucionar los problemas que podrían presentarse cuando crea una conexión de VPC.

Problema

Se produjo un error en la conexión de VPC.

Causa

Esto podría deberse a una de las siguientes causas:

1. El usuario que está creando la conexión de VPC no tiene los permisos correctos para crear un rol vinculado a servicios.

2. Existe un problema de limitación controlada debido a que hay demasiadas solicitudes de IAM; por ejemplo, está utilizando CloudFormation para crear permisos y roles.
3. La cuenta tiene el rol vinculado al servicio y el rol vinculado al servicio se ha modificado.
4. La puerta de enlace de tránsito no está en el estado `available`.

Solución

Según la causa, intente lo siguiente:

1. Compruebe que el usuario tenga los permisos correctos para crear roles vinculados a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM. Una vez que el usuario tenga los permisos, cree la conexión de VPC.
2. Cree la conexión de VPC manualmente. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
3. Compruebe que el rol vinculado al servicio tenga los permisos correctos. Para obtener más información, consulte the section called “Puerta de enlace de tránsito”.
4. Compruebe que la puerta de enlace de tránsito esté en el estado `available`. Para obtener más información, consulte the section called “Consultar una puerta de enlace de tránsito”.

Vinculaciones de funciones de red de AWS Transit Gateway

Puede crear una vinculación de función de red para conectar directamente su puerta de enlace de tránsito directamente con AWS Network Firewall. Elimina la necesidad de crear y administrar las VPC de inspección.

Con una vinculación de firewall, AWS aprovisiona y administra de manera automática todos los recursos necesarios entre bastidores. Verá una nueva conexión de puerta de enlace de tránsito en lugar de puntod de conexión de firewall individualrd. Esto simplifica el proceso de implementación de la inspección centralizada del tráfico de la red.

Para poder utilizar una vinculación de firewall, primero debe crearla en AWS Network Firewall. Para conocer los pasos necesarios para crear la vinculación, consulte Introducción a la administración de AWS Network Firewall en la Guía para desarrolladores de AWS Network Firewall. Una vez creado el firewall, podrá ver el adjunto en la consola de la puerta de enlace de tránsito, en la sección Vinculaciones. La vinculación aparecerá junto con un tipo de función de red.

Temas

- Aceptar o rechazar un adjunto a la función de red AWS Transit Gateway
- Ver adjuntos a las funciones de red de AWS Transit Gateway
- Enrute el tráfico a través de un adjunto de función de red AWS Transit Gateway

Aceptar o rechazar un adjunto a la función de red AWS Transit Gateway

Puede utilizar la consola de Amazon VPC o la AWS Network Firewall CLI o la API para aceptar o rechazar un adjunto de función de red de Transit Gateway, incluidos los adjuntos de Network Firewall. Si usted es el propietario de una puerta de enlace de tránsito y alguien ha creado una vinculación de firewall hacia su puerta de enlace de tránsito desde otra cuenta, debe aceptar o rechazar la solicitud de vinculación.

Para aceptar o rechazar un adjunto a una función de red mediante la CLI de Network Firewall, consulte `AcceptNetworkFirewallTransitGatewayAttachment` o `RejectNetworkFirewallTransitGatewayAttachment` APIs en la Referencia de la AWS Network Firewall API.

Aceptar o rechazar una conexión de función de red mediante la consola

Utilice la consola de Amazon VPC para aceptar o rechazar una conexión de función de red de puerta de enlace de tránsito.

Para aceptar o rechazar una conexión de función de red mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puertas de enlace de tránsito.
3. Elija Conexiones de puerta de enlace de tránsito.
4. Seleccione la conexión con el estado Pendiente de aceptación y un tipo de función de red.
5. Seleccione Acciones y, a continuación, elija Aceptar conexión o Rechazar conexión.
6. En el cuadro de diálogo de confirmación, elija Aceptar o Rechazar.

Si acepta la conexión, se activa y el firewall puede inspeccionar el tráfico. Si rechaza la conexión, pasará a un estado de rechazo y, finalmente, se eliminará.

Ver adjuntos a las funciones de red de AWS Transit Gateway

Puede ver los archivos adjuntos de las funciones de red, incluidos AWS Network Firewall los adjuntos, mediante la consola Amazon VPC o la consola Network Manager para obtener una representación visual de la topología de la red.

Consultar una vinculación de función de red mediante la consola Network Manager

Puede consultar una vinculación de función de red mediante la consola Network Manager.

Para consultar las vinculaciones del firewall en Network Manager

1. Abra la consola de Network Manager en https://console.aws.amazon.com/networkmanager/casa/.
2. Cree una red global en Network Manager si todavía no tiene una.
3. Registrar la puerta de enlace de tránsito en Network Manager.
4. En Redes globales, elige la red global en la que se encuentra la vinculación.
5. En el panel de navegación, seleccione Transit gateways (Puertas de enlace de tránsito).
6. Seleccione la puerta de enlace de tránsito cuyas vinculaciones desea ver.
7. Elija la vista Árbol de topología. Las vinculaciones de Network Firewall aparecen con un icono de función de red.
8. Para ver los detalles sobre una vinculación de firewall específica, seleccione la puerta de enlace de tránsito en la vista de topología y, a continuación, seleccione la pestaña Función de red.

La consola de Network Manager proporciona información detallada sobre las vinculaciones del firewall, incluido su estado, la puerta de enlace de tránsito asociada y las zonas de disponibilidad.

Consultar una vinculación de función de red mediante la consola Amazon VPC

Use la consola de VPC para ver una lista de los tipos de conexiones de puerta de enlace de tránsito

Para consultar los tipos de conexiones de puerta de enlace de tránsito mediante la consola de VPC

- Consulte Consultar una conexión de VPC.

Enrute el tráfico a través de un adjunto de función de red AWS Transit Gateway

Tras crear una conexión de función de red, se deben actualizar las tablas de enrutamiento las puertas de enlace de tránsito para enviar el tráfico a través del firewall para su inspección mediante la consola de Amazon VPC o mediante la CLI. Para conocer los pasos para actualizar una asociación de tabla de enrutamiento de puerta de enlace de tránsito, consulte Asociar una tabla de enrutamiento de la puerta de enlace de tránsito.

Dirija el tráfico a través de una vinculación de firewall mediante la consola

Utilice la consola de Amazon VPC Console para enrutar el tráfico a través de una conexión de función de red de la puerta de enlace.

Para enrutar el tráfico a través de una conexión de función de red mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Puertas de enlace de tránsito.
3. Elija Crear tablas de enrutamiento de puertas de enlace de tránsito.
4. Seleccione la tabla de enrutamiento que desea modificar.
5. Elija Acciones y, a continuación, seleccione Crear enrutamiento estático.
6. Para CIDR, introduzca el bloque de CIDR de destino para el enrutamiento.
7. En Vinculación, seleccione la conexión de función de red. Por ejemplo, podría ser un AWS Network Firewall archivo adjunto.
8. Elija Create static route (Crear ruta estática).

> **Note**
>
> Solo se admiten enrutamientos estáticos.

El tráfico que coincida con el bloque de CIDR de su tabla de enrutamiento ahora se enviará a la vinculación del firewall para su inspección antes de reenviarlo a su destino final.

Para enrutar el tráfico a través de una conexión de función de red mediante la CLI o la API

Utilice la línea de comandos o la API para enrutar una vinculación de red de puerta de enlace de tránsito.

Para enrutar el tráfico a través de una conexión de función de red mediante la línea de comandos o de la API

- Utilice `create-transit-gateway-route`.

  Por ejemplo, la solicitud podría ser para enrutar una vinculación de firewall de red:

```
aws ec2 create-transit-gateway-route \
  --transit-gateway-route-table-id tgw-rtb-0123456789abcdef0 \
  --destination-cidr-block 0.0.0.0/0 \
  --transit-gateway-attachment-id tgw-attach-0123456789abcdef0
```

  Entonces, el resultado devuelve:

```
{
  "Route": {
    "DestinationCidrBlock": "0.0.0.0/0",
    "TransitGatewayAttachments": [
      {
        "ResourceId": "network-firewall",
        "TransitGatewayAttachmentId": "tgw-attach-0123456789abcdef0",
        "ResourceType": "network-function"
      }
    ],
    "Type": "static",
    "State": "active"
  }
}
```

El tráfico que coincida con el bloque de CIDR de su tabla de enrutamiento ahora se enviará a la vinculación del firewall para su inspección antes de reenviarlo a su destino final.

AWS Site-to-Site VPN archivos adjuntos en AWS Transit Gateway

Puede conectar un adjunto de Site-to-Site VPN a una puerta de enlace de tránsito en AWS Transit Gateway, lo que le permitirá conectar sus VPC y redes locales. Tanto las rutas dinámicas como las estáticas son compatibles, así como IPv4 e IPv6.

Requisitos

- Para vincular una conexión de VPN a la puerta de enlace de tránsito debe especificar la puerta de enlace de cliente de VPN, que tiene requisitos de dispositivo específicos. Antes de crear un adjunto de Site-to-Site VPN, revisa los requisitos de la puerta de enlace del cliente para asegurarte de que la puerta de enlace esté configurada correctamente. Para obtener más información sobre estos requisitos, incluidos ejemplos de archivos de configuración de la puerta de enlace, consulte los requisitos para su dispositivo de puerta de enlace Site-to-Site VPN para clientes en la Guía del AWS Site-to-Site VPN usuario.
- Para VPN estáticas, primero tendrá que agregar las rutas estáticas a la tabla de enrutamiento de la puerta de enlace de tránsito. La VPN no filtra las rutas estáticas de una tabla de rutas de una puerta de enlace de tránsito que se dirigen a un adjunto de la Site-to-Site VPN, ya que esto podría permitir un flujo de tráfico saliente no deseado cuando se utiliza una BGP-based VPN. Para conocer los pasos para agregar una ruta estática a la tabla de enrutamiento de una puerta de enlace de tránsito, consulte Crear una ruta estática.

Puede crear, ver o eliminar un adjunto de Site-to-Site VPN de Transit Gateway mediante la consola de Amazon VPC o mediante la CLI AWS .

Tareas

- Cree una pasarela de tránsito adjunta a una VPN en AWS Transit Gateway
- Ver un adjunto de VPN en AWS Transit Gateway
- Eliminar un adjunto de VPN en AWS Transit Gateway

Cree una pasarela de tránsito adjunta a una VPN en AWS Transit Gateway

Para crear una vinculación de la 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 Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Elija Create transit puerta de enlace attachment (Crear conexión de puerta de enlace de tránsito).
4. En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito para la conexión. Puede elegir una puerta de enlace de tránsito de su propiedad.
5. En Attachment type (Tipo de vinculación), elija VPN.
6. En Customer Gateway (Puerta de enlace de cliente), realice alguna de las siguientes operaciones:
   - Para utilizar una puerta de enlace de cliente ya existente, elija Existing (Existente) y, a continuación, seleccione la puerta de enlace que desea utilizar.

     Si la pasarela de tu cliente se encuentra detrás de un dispositivo de traducción de direcciones de red (NAT) que está habilitado para el cruce de NAT (NAT-T), usa la dirección IP pública de tu dispositivo NAT y ajusta las reglas del firewall para desbloquear el puerto UDP 4500.
   - Para crear una puerta de enlace de cliente, elija New (Nueva) y, en IP Address (Dirección IP), escriba una dirección IP pública estática y el BGP ASN.

     En Routing options (Opciones de direccionamiento), elija Dynamic (Dinámico) o Static (Estático). Para obtener más información, consulte las opciones de enrutamiento de Site-to-Site VPN en la Guía del AWS Site-to-Site VPN usuario.
7. En Tunnel Options (Opciones de túnel), introduzca los rangos de CIDR y las claves previamente compartidas del túnel. Para obtener más información, consulte Arquitecturas de Site-to-Site VPN.
8. Elija Create transit gateway attachment (Crear conexión de puerta de enlace de tránsito).

Para crear un adjunto de VPN mediante el AWS CLI

Utilice el comando create-vpn-connection.

Ver un adjunto de VPN en AWS Transit Gateway

Para ver las vinculaciones de VPN mediante la consola

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

2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. En la columna Resource type (Tipo de recurso), busque VPN (VPN). Se trata de las conexiones de VPN.
4. Elija una vinculación para ver los detalles correspondientes o agregar etiquetas.

Para ver los archivos adjuntos de la VPN mediante el AWS CLI

Utilice el comando describe-transit-gateway-attachments.

Eliminar un adjunto de VPN en AWS Transit Gateway

Para eliminar una vinculación de VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la vinculación de VPN.
4. Elija el ID de recurso de la conexión de VPN para navegar hasta la página VPN Connections (Conexiones de VPN).
5. Elija Actions (Acciones), Delete (Eliminar).
6. Cuando se le pida confirmación, elija Eliminar.

Para eliminar un adjunto de VPN mediante el AWS CLI

Utilice el comando delete-vpn-connection.

Archivos adjuntos de VPN Concentrator en AWS Transit Gateway

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

Cómo funciona VPN Concentrator

Un concentrador VPN aparece como un único adjunto en tu pasarela de tránsito, pero puede alojar varias conexiones Site-to-Site VPN.

El tráfico de todas las conexiones VPN del Concentrator se enruta a través del mismo adjunto a la pasarela de tránsito, lo que le permite aplicar políticas de enrutamiento y reglas de seguridad coherentes en todos los sitios conectados. El Concentrator se integra perfectamente con las tablas de rutas de las pasarelas de tránsito, lo que le permite controlar el flujo de tráfico entre sus sitios remotos y otros archivos adjuntos VPCs, como otras conexiones VPN y conexiones entre pares.

Ventajas del concentrador VPN

- Optimización de costos: reduzca los costos al consolidar varias conexiones VPN de bajo ancho de banda en un único accesorio de pasarela de tránsito, lo que resulta especialmente beneficioso cuando los sitios individuales no requieren toda la capacidad de conexión de la VPN.
- Administración simplificada: administre las conexiones de varios sitios remotos a través de un accesorio unificado y, al mismo tiempo, mantenga el control y la supervisión de las conexiones VPN individuales.
- Enrutamiento coherente: aplique políticas de enrutamiento unificadas en todos los sitios conectados mediante una única asociación de tablas de rutas de la pasarela de tránsito.
- Arquitectura escalable: Conecte hasta 100 sitios remotos mediante un solo concentrador, con soporte para hasta 5 concentradores por puerta de enlace de tránsito.
- Características de VPN estándar: cada conexión VPN admite las mismas capacidades de seguridad, supervisión y enrutamiento que las conexiones Site-to-Site VPN estándar.

Requisitos y limitaciones

- Solo enrutamiento BGP: VPN Concentrator solo admite el enrutamiento BGP (dinámico). No se admite el enrutamiento estático en el momento del lanzamiento.
- Requisitos de puerta de enlace para el cliente: cada sitio remoto requiere una puerta de enlace para el cliente que admita el enrutamiento BGP. Antes de crear conexiones VPN en un concentrador, revise los requisitos de la puerta de enlace para clientes en la sección Requisitos para su dispositivo de puerta de enlace para clientes Site-to-Site VPN de la Guía del AWS Site-to-Site VPN usuario.

- Consideraciones de rendimiento: cada conexión VPN de un concentrador está diseñada para un ancho de banda máximo de 100 Mbps. Para requisitos de ancho de banda más altos, considere la posibilidad de utilizar adjuntos VPN de pasarela de tránsito estándar.

Puede crear, ver o eliminar un adjunto a un concentrador de VPN mediante la consola de AWS VPC o la CLI. AWS Las conexiones VPN individuales del Concentrator se administran a través de la conexión VPN estándar APIs y las interfaces de consola.

Tareas

- Crear un adjunto de VPN Concentrator en AWS Transit Gateway
- Ver un adjunto de VPN Concentrator en AWS Transit Gateway
- Eliminar un adjunto de VPN Concentrator en AWS Transit Gateway

Crear un adjunto de VPN Concentrator en AWS Transit Gateway

Requisitos previos

- Debe tener una pasarela de tránsito existente en su cuenta.

Para crear un adjunto a un concentrador 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) Para añadir etiquetas adicionales, selecciona Añadir nueva etiqueta y especifica la clave y el valor de cada etiqueta.
7. Elija Crear concentrador de Site-to-Site VPN.

Tras crear el adjunto al concentrador VPN, éste aparecerá en la lista de adjuntos con el tipo de recurso del concentrador VPN y el estado inicial pendiente. Cuando el adjunto esté listo, el

estado cambiará a Disponible. A continuación, puede crear conexiones Site-to-Site VPN en este concentrador.

Para crear un adjunto a un concentrador VPN mediante el AWS CLI

Utilice el comando create-vpn-concentrator.

Para crear una conexión VPN en un concentrador VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones Site-to-Site VPN.
3. Elija Create VPN Connection (Crear conexión VPN).
4. Para el tipo de puerta de enlace de destino, elija Site-to-Site VPN Concentrator.
5. Para el concentrador de Site-to-Site VPN, elija el concentrador de VPN en el que desee crear la conexión VPN.
6. En Customer Gateway (Puerta de enlace de cliente), realice alguna de las siguientes operaciones:
   - Para utilizar una puerta de enlace de cliente ya existente, elija Existing (Existente) y, a continuación, seleccione la puerta de enlace que desea utilizar. Asegúrese de que la pasarela del cliente sea compatible con el enrutamiento BGP.
   - Para crear una gateway de cliente, elija New (Nuevo). En Dirección IP, introduzca la dirección IP pública estática del dispositivo de puerta de enlace del cliente. Para BGP ASN, introduzca el número de sistema autónomo (ASN) del Border Gateway Protocol (BGP) para su pasarela de cliente.

     Si su puerta de enlace 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.
7. Para las opciones de enrutamiento, se selecciona automáticamente el modo dinámico (requiere BGP). VPN Concentrator solo admite el enrutamiento dinámico con BGP.
8. Para almacenar claves previamente compartidas, selecciona Standard o Secrets Manager.
9. Para el ancho de banda del túnel, se selecciona automáticamente el estándar. El concentrador VPN solo admite el ancho de banda de túnel estándar.
10. Para la versión Tunnel inside IP, seleccione una IPv4o IPv6.
11. (Opcional) Seleccione Activar la aceleración para mejorar el rendimiento de los túneles VPN.

12. (Opcional) Para el CIDR IPv4 de red local, proporcione un rango de IPv4 CIDR.
13. (Opcional) Para el CIDR de IPv4 red remota, proporcione un IPv4 rango de CIDR.
14. Para el tipo de dirección IP externa, puede seleccionar Pública IPv4 o IPv6Dirección.
15. (Opcional) En el caso de las opciones de túnel, puede configurar los ajustes del túnel, como las direcciones IP internas del túnel y las claves previamente compartidas. Para obtener más información, consulte las arquitecturas de Site-to-Site VPN en la Guía del AWS Site-to-Site VPN usuario.
16. (Opcional) Para añadir etiquetas adicionales, elija Añadir nueva etiqueta y especifique la clave y el valor de cada etiqueta.
17. Elija Create VPN Connection (Crear conexión VPN).

La conexión VPN aparece en la lista de conexiones VPN con el ID del concentrador de VPN en la columna ID de Transit Gateway y un estado inicial de Pendiente. Cuando la conexión VPN esté lista, el estado cambiará a Disponible.

Para crear una conexión VPN en un concentrador VPN mediante el AWS CLI

Utilice el create-vpn-connectioncomando y especifique el ID del concentrador VPN mediante el `--vpn-concentrator-id` parámetro.

Ver un adjunto de VPN Concentrator en AWS Transit Gateway

Para ver los archivos adjuntos de su concentrador 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 Transit Gateways Attachments (Conexiones de puerta de enlace de tránsito).
3. En la columna Tipo de recurso, busca VPN Concentrator. Estos son los archivos adjuntos del concentrador VPN.
4. Seleccione una vinculación para ver sus detalles.

Para ver las conexiones VPN en un concentrador VPN mediante la consola

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

3. En la lista de conexiones VPN, identifique las conexiones que muestren un ID de VPN Concentrator en la columna Transit Gateway ID. Estas son las conexiones VPN alojadas en los concentradores VPN.
4. Elija una conexión VPN para ver sus detalles.

Para ver los archivos adjuntos de su concentrador VPN mediante el AWS CLI

Utilice el describe-vpn-concentratorcomando para ver los detalles del concentrador VPN o utilice el describe-transit-gateway-attachmentscomando con un filtro para el tipo de recurso. `vpn-concentrator`

Para ver las conexiones VPN en un concentrador VPN mediante el AWS CLI

Utilice el describe-vpn-connectionscomando con un filtro `vpn-concentrator-id` para ver las conexiones VPN asociadas a un concentrador específico.

Eliminar un adjunto de VPN Concentrator en AWS Transit Gateway

Requisitos previos

- Se deben eliminar todas las conexiones VPN del concentrador VPN antes de poder eliminar el adjunto del concentrador.
- Asegúrese de haber actualizado las configuraciones de enrutamiento para tener en cuenta la eliminación del concentrador VPN y sus conexiones VPN asociadas.

Para eliminar las conexiones VPN en un concentrador VPN mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Conexiones Site-to-Site VPN.
3. Identifique las conexiones VPN asociadas a su concentrador de VPN buscando el ID del concentrador de VPN en la columna de ID de Transit Gateway.
4. Seleccione la conexión VPN que desee eliminar.
5. Seleccione Acciones, Eliminar.
6. Cuando se le pida confirmación, elija Eliminar.
7. Repita los pasos 4 a 6 para cada conexión VPN asociada al concentrador VPN.

Para eliminar un archivo adjunto al concentrador 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 Transit Gateways Attachments (Conexiones de puerta de enlace de tránsito).
3. Seleccione el adjunto del concentrador VPN que desee eliminar. Compruebe que no haya ninguna conexión VPN asociada a este concentrador.
4. Seleccione Acciones y elimine el archivo adjunto.
5. Cuando se le pida confirmación, seleccione Eliminar.

El archivo adjunto del VPN Concentrator pasa al estado de eliminación y se eliminará de su cuenta. Este proceso puede tardar unos minutos en completarse.

Para eliminar las conexiones VPN en un concentrador VPN mediante el AWS CLI

Utilice el delete-vpn-connectioncomando para cada conexión VPN asociada al concentrador VPN.

Para eliminar un archivo adjunto al concentrador VPN mediante el AWS CLI

Utilice el delete-vpn-concentratorcomando después de eliminar todas las conexiones VPN.

Archivos adjuntos de Client VPN en AWS Transit Gateway

Al asociar un punto de conexión Client VPN a una puerta de enlace de tránsito, se crea automáticamente un adjunto de Client VPN que le permite enrutar el tráfico entre sus VPC, las redes locales y los puntos de enlace de Client VPN. AWS Transit Gateway admite adjuntos de Client VPN multicuenta, lo que permite a las cuentas con las que se comparte la pasarela de tránsito crear sus propios adjuntos de Client VPN.

Una vez que el punto de conexión Client VPN esté asociado a una pasarela de tránsito, podrá ver el adjunto en la consola de Transit Gateway, en Adjuntos de Transit Gateway. El archivo adjunto aparecerá junto con un tipo de Client VPN.

Requisitos y limitaciones

- Su puerta de enlace de tránsito debe tener un bloque CIDR de IPv4 o IPv6 asignado antes de poder crear un adjunto de Client VPN.

- La propagación de la tabla de rutas debe estar habilitada para los archivos adjuntos de Client VPN para permitir el tráfico entre el punto final de Client VPN y la puerta de enlace de tránsito. Consulte Habilitar la propagación de rutas.

Tareas

- Crear un adjunto de Client VPN en AWS Transit Gateway
- Ver un adjunto de Client VPN en AWS Transit Gateway
- Eliminar un adjunto de Client VPN en AWS Transit Gateway
- Aceptar o rechazar un adjunto de Client VPN en AWS Transit Gateway

Crear un adjunto de Client VPN en AWS Transit Gateway

Requisitos previos

- Debe tener una pasarela de tránsito existente en su cuenta.
- Tu pasarela de transporte público debe tener un bloque CIDR de IPv4 o IPv6 asignado.

Se crea automáticamente un adjunto de Client VPN al asociar un punto final de Client VPN a una puerta de enlace de tránsito.

Para crear un adjunto de Client 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 los puntos finales de Client VPN.
3. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).
4. Seleccione Transit Gateway como tipo de asociación e introduzca el ID de Transit Gateway que desee utilizar.
5. Elija Create Client VPN endpoint (Crear punto de conexión de Client VPN).

Tras crear el adjunto de Client VPN, aparece en la lista de adjuntos con un tipo de recurso de Client VPN y un estado inicial de Pendiente. Cuando el adjunto esté listo, el estado cambiará a Disponible. Si la pasarela de transporte está en una cuenta diferente, el estado del archivo adjunto es Pendiente de aceptación hasta que el propietario de la pasarela de transporte lo acepte.

Para obtener más información sobre la creación de puntos de conexión Client VPN, consulte Introducción a AWS Client VPN.

Para crear un adjunto de Client VPN mediante el AWS CLI

Utilice el comando create-client-vpn-endpoint.

Ver un adjunto de Client VPN en AWS Transit Gateway

Para ver los archivos adjuntos de Client 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 Transit Gateways (Puertas de enlace de tránsito).
3. Elija Conexiones de puerta de enlace de tránsito.
4. En la columna Tipo de recurso, busca Client VPN.
5. Seleccione una vinculación para ver sus detalles.

Para ver los archivos adjuntos de Client VPN mediante el AWS CLI

Utilice el comando describe-transit-gateway-attachments con un filtro por tipo de recurso. `client-vpn`

Eliminar un adjunto de Client VPN en AWS Transit Gateway

Para eliminar un adjunto de Client 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 Transit Gateways (Puertas de enlace de tránsito).
3. Elija Conexiones de puerta de enlace de tránsito.
4. Seleccione el adjunto de Client VPN que desee eliminar.
5. Elija Actions (Acciones),Delete transit gateway attachment (Eliminar conexión de puerta de enlace de tránsito).
6. Cuando se le pida confirmación, ingrese **`delete`** y elija Eliminar.

El archivo adjunto de Client VPN pasa al estado de eliminación y se eliminará de su cuenta. Este proceso puede tardar algún tiempo en completarse.

Para eliminar un adjunto de Client VPN mediante el AWS CLI

Utilice el comando delete-transit-gateway-client-vpn-attachment.

Aceptar o rechazar un adjunto de Client VPN en AWS Transit Gateway

Si un terminal Client VPN de otra cuenta crea un adjunto en tu pasarela de tránsito, debes aceptar o rechazar la solicitud de adjunto para que el tráfico pueda fluir.

Para aceptar o rechazar un adjunto de Client 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 Transit Gateways (Puertas de enlace de tránsito).
3. Elija Conexiones de puerta de enlace de tránsito.
4. Seleccione el archivo adjunto con un estado de Aceptación pendiente y un tipo de Client VPN.
5. Seleccione Acciones y, a continuación, elija Aceptar conexión o Rechazar conexión.
6. En el cuadro de diálogo de confirmación, elija Aceptar o Rechazar.

Si acepta el adjunto, se activará y AWS Transit Gateway empezará a procesar el tráfico hacia y desde el punto de conexión Client VPN. Si rechaza la conexión, pasará a un estado de rechazo y, finalmente, se eliminará.

Para aceptar un adjunto de Client VPN mediante el AWS CLI

Utilice el comando accept-transit-gateway-client-vpn-attachment.

Para rechazar un adjunto de Client VPN mediante el AWS CLI

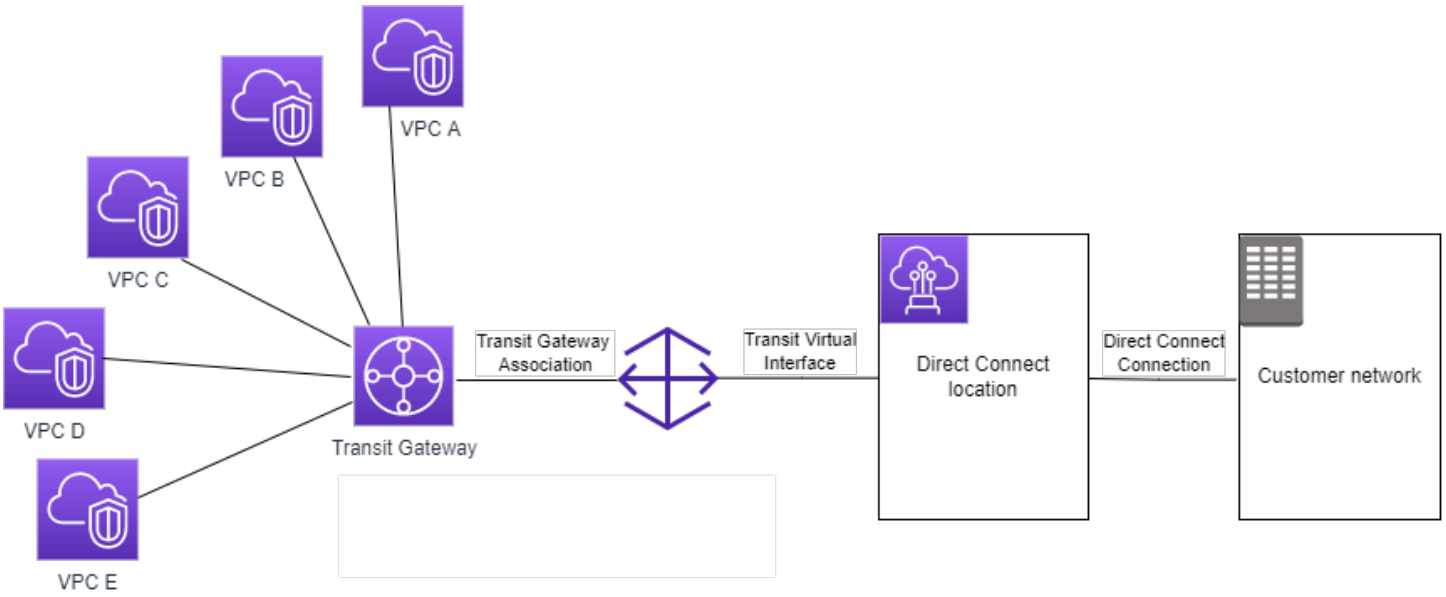
Utilice el comando reject-transit-gateway-client-vpn-attachment.

Conexiones de puerta de enlace de tránsito a una puerta de enlace de Direct Connect en AWS Transit Gateway

Asocie una gateway de tránsito a una gateway de Direct Connect con una interfaz virtual de tránsito. Esta configuración ofrece los siguientes beneficios. Puede hacer lo siguiente:

- Administrar una única conexión para las distintas VPC o VPN que haya en la misma región.
- Publicar los prefijos desde las instalaciones hasta AWS y desde AWS hasta las instalaciones.

El siguiente diagrama muestra cómo le permite la gateway de Direct Connect crear una única conexión con su conexión de Direct Connect que todas las VPC pueden utilizar.



La solución implica los siguientes componentes:

- Una gateway de tránsito.
- Una gateway de Direct Connect.
- Una asociación entre la puerta de enlace de Direct Connect y la puerta de enlace de tránsito.
- Una interfaz virtual de tránsito vinculada a la gateway de Direct Connect.

Para obtener información sobre la configuración de gateways de Direct Connect con gateways de tránsito, consulte Asociaciones de gateway de tránsito en la Guía del usuario de AWS Direct Connect.

Vinculaciones de interconexiones de la puerta de enlace de tránsito en AWS Transit Gateway

Puede interconectar dos puerta de enlaces de tránsito en forma intrarregional e interregional, y enrutar el tráfico entre ellas, incluidos el tráfico IPv4 e IPv6. Para ello, cree un archivo adjunto de interconexión en la puerta de enlace de tránsito y especifique una puerta de enlace de tránsito. La puerta de enlace de tránsito de interconexión puede estar en su cuenta o provenir de otra cuenta diferente. También se puede solicitar una vinculación de interconexión desde su cuenta a una puerta de enlace de transporte de otra cuenta.

Después de crear una solicitud de vinculación de interconexión, el propietario de la puerta de enlace de tránsito del mismo nivel (también conocida como la puerta de enlace de tránsito del aceptador) debe aceptar la solicitud. Para enrutar el tráfico entre las puerta de enlaces de tránsito, agregue una ruta estática a la tabla de enrutamiento de la puerta de enlace de tránsito que apunte hacia la interconexión de la puerta de enlace de tránsito.

Se recomienda utilizar ASN únicos para que cada puerta de enlace de tránsito interconectada aproveche las capacidades futuras de propagación de rutas.

La interconexión de la puerta de enlace de tránsito no es compatible con la resolución de nombres de host DNS IPv4 públicos o privados en direcciones IPv4 privadas a través de VPC en ambos lados de la vinculación de la interconexión de la puerta de enlace de tránsito con Amazon Route 53 Resolver en otra Región. Para obtener más información acerca de Route 53 Resolver, consulte Qué es Route 53 Resolver? en la Guía del desarrollador de Amazon Route 53.

El emparejamiento de puerta de enlace entre regiones utiliza la misma infraestructura de red que un emparejamiento de VPC. Por lo tanto, el tráfico está cifrado mediante el cifrado AES-256 en la capa de red virtual a medida que se desplaza entre las regiones. El tráfico también está cifrado mediante el cifrado AES-256 en la capa física cuando atraviesa enlaces de red que están fuera del control físico de AWS. Como resultado, el tráfico tiene un doble cifrado en los enlaces de red fuera del control físico de AWS. Dentro de la misma región, el tráfico también está cifrado en la capa física solo cuando atraviesa enlaces de red que están fuera del control físico de AWS.

Para obtener información sobre las regiones que admiten vinculaciones de interconexiones de puerta de enlace de tránsito, consulte Preguntas frecuentes de AWS Transit Gateways.

Consideraciones sobre la región de AWS registrada

Puede interconectar las puerta de enlaces de tránsito a través de los límites de la región registrada. Para obtener información sobre estas regiones y cómo elegirlas, consulte Gestión de regiones de AWS. Tenga en cuenta lo siguiente cuando utilice la interconexión de la puerta de enlace de tránsito en estas regiones:

- Puede hacer una interconexión en una región registrada siempre y cuando la cuenta que acepte la vinculación de la interconexión haya elegido esa región.
- Independientemente del estado de elección de la región, AWS comparte los siguientes datos de cuenta con la cuenta que acepta la vinculación de la interconexión:
  - Cuenta de AWSID de

  - ID de puerta de enlace de tránsito
  - Código de región
- Cuando elimina la vinculación de la puerta de enlace de tránsito, se eliminan los datos de cuenta anteriores.
- Recomendamos que elimine el archivo adjunto de la interconexión de la puerta de enlace de tránsito antes de dejar de elegir la región. Si no elimina la vinculación de la interconexión, es posible que el tráfico continúe pasando por el archivo adjunto y siga incurriendo en cargos. Si no elimina el archivo adjunto, puede volver a elegirlo y, a continuación, eliminarlo.
- En general, la puerta de enlace de tránsito tiene un modelo de pago de remitente. Al utilizar una vinculación de interconexión de puerta de enlace de tránsito a través de un límite de elección, puede incurrir en cargos en una región que acepte la vinculación, incluidas aquellas regiones que no se haya registrado. Para obtener más información, consulte Precio de AWS Transit Gateway.

Tareas

- Creación de una vinculación de interconexión de una AWS Transit Gateway
- Acepte o rechace una solicitud de vinculación de interconexión de AWS Transit Gateway
- Agregue una ruta a una tabla de rutas de Transit Gateway mediante AWS Transit Gateway
- Para eliminar una vinculación de interconexión de AWS Transit Gateway

Creación de una vinculación de interconexión de una AWS Transit Gateway

Antes de empezar, asegúrese de que tiene el ID de la puerta de enlace de tránsito que desea asociar. Si la puerta de enlace de tránsito se encuentra en otra Cuenta de AWS, asegúrese de que tiene el ID de Cuenta de AWS del propietario de la puerta de enlace de tránsito. Después de crear la vinculación de interconexión, el propietario de la puerta de enlace de tránsito del aceptador debe aceptar o rechazar la solicitud de conexión.

Para crear una vinculación de interconexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Elija Create transit puerta de enlace attachment (Crear conexión de puerta de enlace de tránsito).

4. En Transit Gateway ID (ID de puerta de enlace de tránsito), elija la puerta de enlace de tránsito para la conexión. Puede elegir una puerta de enlace de tránsito de su propiedad. Las puertas de enlace de tránsito que se comparten con usted no están disponibles para la interconexión.
5. Para Attachment type (Tipo de vinculación), seleccione Peering Connection (Interconexión).
6. De manera opcional, introduzca una etiqueta de nombre para la vinculación.
7. Para Account (Cuenta), realice una de las siguientes acciones:
   - Si la puerta de enlace de tránsito está en su cuenta, elija My account (Mi cuenta).
   - Si la puerta de enlace de tránsito está en una Cuenta de AWS diferente, elija Other account (Otra cuenta). En Account ID (ID de cuenta), ingrese el ID de la Cuenta de AWS.
8. En Region (Región), elija la región en la que se encuentra la puerta de enlace de tránsito.
9. En Transit puerta de enlace (accepter) (Gateway de tránsito (aceptadora)), ingrese el ID de la puerta de enlace de tránsito que desea conectar.
10. Elija Create transit puerta de enlace attachment (Crear conexión de puerta de enlace de tránsito).

Para crear una vinculación de interconexión mediante la AWS CLI

Utilice el comando create-transit-puerta de enlace-peering-attachment.

Acepte o rechace una solicitud de vinculación de interconexión de AWS Transit Gateway

Cuando se crea una vinculación de interconexión de puerta de enlace de tránsito, se lo hace automáticamente en un estado de `pendingAcceptance` y permanece en este estado indefinidamente hasta que se acepte o rechace. Para activar la vinculación de interconexión, el propietario de la puerta de enlace de tránsito del aceptador debe aceptar la solicitud de vinculación de interconexión, incluso si las dos puertas de enlace de tránsito están en la misma cuenta. Acepte la solicitud de vinculación de interconexión de la región en la que se encuentra la puerta de enlace de tránsito del aceptador. Como alternativa, si se rechaza la vinculación de interconexión, se debe rechazar la solicitud de la región en la que se encuentra la puerta de enlace de tránsito del aceptador.

Para aceptar una solicitud de vinculación de interconexión mediante la consola

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

2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la interconexión de la puerta de enlace de tránsito que está pendiente de aceptación.
4. Elija Actions (Acciones), Accept transit puerta de enlace attachment (Aceptar conexión de puerta de enlace de tránsito).
5. Agregue la ruta estática a la tabla de enrutamiento de la puerta de enlace de tránsito. Para obtener más información, consulte the section called “Crear una ruta estática”.

Para rechazar una solicitud de vinculación de interconexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la interconexión de la puerta de enlace de tránsito que está pendiente de aceptación.
4. Elija Actions (Acciones), Reject transit puerta de enlace attachment (Rechazar conexión de puerta de enlace de tránsito).

Para aceptar o rechazar una vinculación de interconexión utilizando la AWS CLI

Utilice los comandos accept-transit-puerta de enlace-peering-attachment y reject-transit-puerta de enlace-peering-attachment.

Agregue una ruta a una tabla de rutas de Transit Gateway mediante AWS Transit Gateway

Para enrutar el tráfico entre las puerta de enlaces de tránsito interconectadas, debe añadir una ruta estática a la tabla de ruteo de la puerta de enlace de tránsito que apunte al enlace de interconexión de la puerta de enlace de tránsito. El propietario de la puerta de enlace de tránsito del aceptador también debe agregar una ruta estática a la tabla de enrutamiento de la puerta de enlace de tránsito.

Para crear una ruta estática utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento para la que se va a crear una ruta.

4. Elija Actions (Acciones), Create static route (Crear ruta estática).
5. En la página Create static route (Crear ruta estática), ingrese el bloque de CIDR para el que se debe crear la ruta. Por ejemplo, especifique el bloque de CIDR de una VPC que esté conectada a la puerta de enlace de tránsito del mismo nivel.
6. Elija el enlace de interconexión de la ruta.
7. Elija Create static route (Crear ruta estática).

Para crear una ruta estática mediante el AWS CLI

Utilice el comando create-transit-gateway-route.

> **Important**
>
> Después de crear la ruta, la conexión de emparejamiento de la puerta de enlace de tránsito ya debe estar asociada con la tabla de enrutamiento de la puerta de enlace de tránsito. Para obtener más información, consulte the section called “Asociar una tabla de enrutamiento de la puerta de enlace de tránsito”.

Para eliminar una vinculación de interconexión de AWS Transit Gateway

Puede eliminar una interconexión de la puerta de enlace de tránsito. El propietario de cualquiera de las puerta de enlaces de tránsito puede eliminar las vinculaciones.

Para eliminar una vinculación de interconexión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Vinculaciones de las puerta de enlaces de tránsito).
3. Seleccione la interconexión de la puerta de enlace de tránsito.
4. Elija Actions (Acciones),Delete transit puerta de enlace attachment (Eliminar conexión de puerta de enlace de tránsito).
5. Ingrese **`delete`** y elija Delete (Eliminar).

Para eliminar una vinculación de interconexión mediante la AWS CLI

Utilice el comando delete-transit-gateway-peering-attachment.

Conecta archivos adjuntos y conecta a tus compañeros en AWS Transit Gateway

Puede crear un adjunto de Transit Gateway Connect para establecer una conexión entre una pasarela de tránsito y dispositivos virtuales de terceros (como SD-WAN dispositivos) que se ejecutan en una VPC. Una conexión de Connect admite el protocolo de túnel de encapsulación de enrutamiento genérico (GRE) para un alto rendimiento y el protocolo de gateway fronteriza (BGP) para enrutamiento dinámico. Después de crear una conexión de Connect, puede crear uno o más túneles de GRE (también denominados pares de Transit Gateway Connect) en la conexión de Connect para conectar la gateway de tránsito y el dispositivo de terceros. Establece dos sesiones de BGP sobre el túnel de GRE para intercambiar información de enrutamiento.

> **Important**
>
> Un par de Transit Gateway Connect consta de dos sesiones de interconexión de BGP que finalizan en AWS una infraestructura gestionada. Las dos sesiones de interconexión de BGP proporcionan redundancia del plano de enrutamiento, lo que garantiza que perder una sesión de interconexión de BGP no afecte a la operación de enrutamiento. La información de enrutamiento recibida de ambas sesiones de BGP se acumula para el par Connect determinado. Las dos sesiones de interconexión de BGP también protegen contra cualquier operación de infraestructura de AWS como mantenimiento de rutina, aplicación de parches, actualizaciones de hardware y reemplazos. Si su par Connect funciona sin la sesión de interconexión de doble BGP recomendada configurada para la redundancia, es posible que experimente una pérdida momentánea de conectividad durante las operaciones de infraestructura. AWS Se recomienda encarecidamente que configure ambas sesiones de interconexión de BGP en el par de Connect. Si ha configurado varios pares de Connect para que admitan la alta disponibilidad en el lado del dispositivo, le recomendamos que configure ambas sesiones de interconexión de BGP en cada una de sus interconexiones de Connect.

Una conexión de Connect utiliza una conexión de Direct Connect o VPC existente como mecanismo de transporte subyacente. Esto se conoce como conexión de transporte. La gateway de tránsito identifica los paquetes de GRE coincidentes del dispositivo de terceros como tráfico de la conexión de Connect. Trata cualquier otro paquete, incluidos los paquetes de GRE con información incorrecta de origen o destino, como tráfico procedente de la conexión de transporte.

> **Note**
>
> Para usar un accesorio Direct Connect como mecanismo de transporte, primero tendrá que integrar Direct Connect con AWS Transit Gateway. Para conocer los pasos para crear esta integración, consulte Integrar SD-WAN dispositivos con AWS Transit Gateway y Direct Connect.

Pares de Connect

Un par de Connect (túnel de GRE) consta de los siguientes componentes.

Bloques CIDR internos (direcciones de BGP)

Las direcciones IP internas que se utilizan para los pares de BGP. Debe especificar un bloque CIDR /29 del rango `169.254.0.0/16` para IPv4. Si lo desea, puede especificar un bloque CIDR /125 del rango `fd00::/8` para IPv6. Los siguientes bloques de CIDR están reservados y no se pueden utilizar:

- 169,254.0. 0/29
- 169,254.1. 0/29
- 169,254,2. 0/29
- 169,254,3. 0/29
- 169,254,4. 0/29
- 169,254,5. 0/29
- 169.254.169. 248/29

Debe configurar la primera dirección del rango IPv4 del dispositivo como la dirección IP de BGP. Cuando utiliza IPv6, si el bloque CIDR interno es fd00::/125, debe configurar la primera dirección de este rango (fd00::1) en la interfaz del túnel del dispositivo.

Las direcciones de BGP deben ser únicas en todos los túneles de una gateway de tránsito.

Dirección IP del par

La dirección IP del mismo par (dirección IP externa de GRE) en el lado del dispositivo del par de Connect. Puede ser cualquier dirección IP. La dirección IP puede ser una dirección IPv4 o IPv6, pero debe ser la misma familia de direcciones IP que la dirección de gateway de tránsito.

Dirección de gateway de tránsito

La dirección IP del par (dirección IP externa de GRE) en el lado de la gateway de tránsito del par de Connect. La dirección IP debe especificarse desde el bloque CIDR de la gateway de tránsito y debe ser única en las conexiones de Connect en la gateway de tránsito. Si no especifica una dirección IP, utilizaremos la primera dirección disponible del bloque CIDR de la gateway de tránsito.

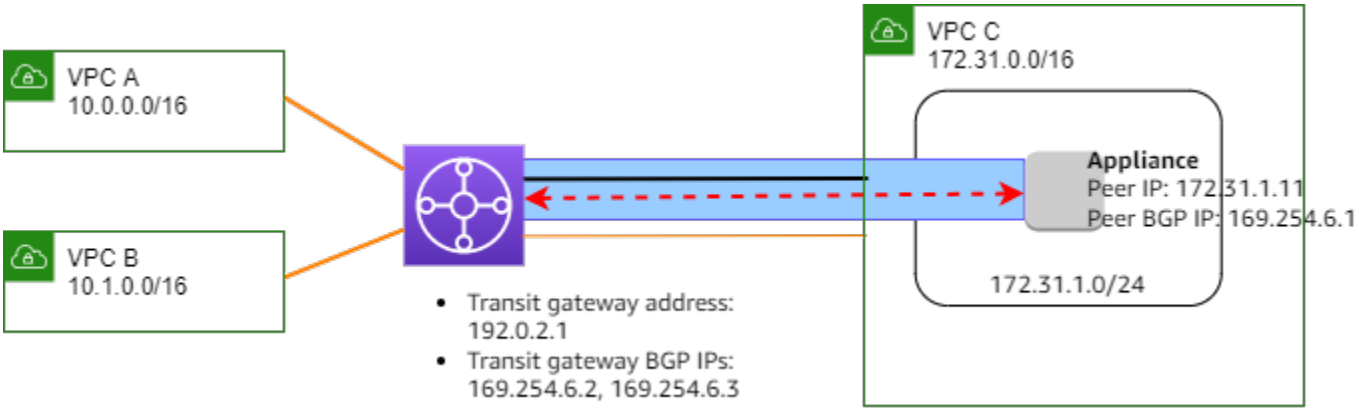
Puede agregar un bloque CIDR de gateway de tránsito cuando crea o modifica una gateway de tránsito.

La dirección IP puede ser una dirección IPv4 o IPv6, pero debe ser la misma familia de direcciones IP que la dirección IP del par.

La dirección IP del par y la dirección de gateway de tránsito se utilizan para identificar de forma única el túnel de GRE. Puede reutilizar cualquiera de las direcciones en varios túneles, pero no ambos en el mismo túnel.

Transit Gateway Connect for the BGP peering solo admite BGP (MP-BGP) multiprotocolo, donde se requiere el direccionamiento Unicast IPv4 para establecer también una sesión de BGP para IPv6 Unicast. Puede utilizar tanto direcciones IPv4 como IPv6 para las direcciones IP externas de GRE.

En el siguiente ejemplo se muestra una conexión de Connect entre una gateway de tránsito y un dispositivo de una VPC.



Componente de diagrama	Description (Descripción)
	Conexión de VPC

Componente de diagrama	Description (Descripción)
	Conexión de Connect
	Túnel de GRE (par de Connect)
	Sesión de pares de BGP

En el ejemplo anterior, se crea una conexión de Connect en una conexión de VPC existente (la conexión de transporte). Se crea un par de Connect en la conexión de Connect para establecer una conexión con un dispositivo en la VPC. La dirección de la gateway de tránsito es `192.0.2.1` y el rango de direcciones de BGP es `169.254.6.0/29`. La primera dirección IP del rango (`169.254.6.1`) se configura en el dispositivo como la dirección IP de BGP del par.

La tabla de enrutamiento de la subred para la VPC C tiene una ruta que apunta el tráfico destinado al bloque CIDR de la gateway de tránsito a la gateway de tránsito.

Destino	Target
172.31.0. 0/16	Local
192.0.2. 0/24	tgw-id

Requisitos y consideraciones

A continuación se detallan los requisitos y consideraciones para una conexión de Connect.

- Para obtener información sobre las regiones que admiten las conexiones de Connect, consulte Preguntas frecuentes de AWS Transit Gateways.
- El dispositivo de terceros debe configurarse para enviar y recibir tráfico a través de un túnel de GRE hacia y desde la gateway de tránsito mediante la conexión de Connect.
- El dispositivo de terceros debe estar configurado a fin de utilizar BGP para actualizaciones de rutas dinámicas y comprobaciones de estado.
- Se admiten los siguientes tipos de BGP:

  - BGP exterior (eBGP): se utiliza para conectarse a enrutadores que se encuentran en un sistema autónomo diferente al de la gateway de tránsito. Si utiliza eBGP, debe configurar ebgp-multihop con un valor de tiempo de vida (TTL) de 2.
  - BGP interior (iBGP): Se utiliza para conectarse a enrutadores que se encuentran en el mismo sistema autónomo que la gateway de tránsito. La puerta de enlace de tránsito no instalará rutas desde un par de iBGP (dispositivo de terceros), a menos que las rutas se originen desde un par de eBGP y deberían tener next-hop-self configurado. Las rutas anunciadas por el dispositivo de terceros a través de los pares de iBGP deben tener un ASN.
  - MP-BGP (extensiones multiprotocolo para BGP): se utiliza para admitir varios tipos de protocolos, como las familias de direcciones IPv4 e IPv6.
- El tiempo de espera predeterminado de mantenimiento BGP es de 10 segundos y el temporizador de retención predeterminado es de 30 segundos.
- No se admite el emparejamiento BGP de IPv6; solo se admite el emparejamiento de BGP. IPv4-based Los prefijos de IPv6 se intercambian mediante el emparejamiento BGP de IPv4 mediante. MP-BGP
- No se admite Bidirectional Forwarding Detection (BFD).
- No se admite el reinicio de gracia de BGP.
- Cuando crea un par de gateway de tránsito, si no especifica un número de ASN del par, seleccionaremos el número de ASN de la gateway de tránsito. Esto significa que el dispositivo y la gateway de tránsito estarán en el mismo sistema autónomo que realiza iBGP.
- Un par de Connect que utilice el AS-PATH atributo BGP es la ruta preferida cuando hay dos pares de Connect.

  Para utilizar el enrutamiento de rutas múltiples (ECMP) de igual costo entre varios dispositivos, debe configurar el dispositivo para que anuncie los mismos prefijos en la puerta de enlace de tránsito con el mismo atributo de BGP. AS-PATH Para que la pasarela de tránsito elija todas las rutas ECMP disponibles, el número de sistema autónomo (ASN) AS-PATH y el número de sistema autónomo (ASN) deben coincidir. La gateway de tránsito puede usar ECMP entre pares de Connect de la misma conexión de Connect o entre conexiones de Connect en la misma gateway de tránsito. La gateway de tránsito no puede utilizar el ECMP en dos pares de BGP redundantes si está establecido en un único par.
- Con una conexión de Connect, las rutas se propagan a una tabla de enrutamiento de gateway de tránsito de forma predeterminada.
- No se admiten rutas estáticas.

- Configure la MTU del túnel GRE para que sea más pequeña que la MTU de la interfaz externa restando la sobrecarga del encabezado GRE (4 bytes) y del encabezado IP externo (20 bytes). Por ejemplo, si la MTU de la interfaz externa es de 1500 bytes, establece la MTU del túnel GRE en 1476 bytes (1500 - 4 - 20 = 1476) para evitar la fragmentación de los paquetes.

Tareas

- Crear una conexión de Connect en AWS Transit Gateway
- Creación de un emparejamiento en AWS Transit Gateway
- Vea los archivos adjuntos de Connect y los compañeros de Connect en AWS Transit Gateway
- Modifique el archivo adjunto Connect y las etiquetas de pares Connect en AWS Transit Gateway
- Eliminar un emparejamiento en AWS Transit Gateway
- Eliminar una conexión de Connect en AWS Transit Gateway

Crear una conexión de Connect en AWS Transit Gateway

Para crear una conexión de Connect, debe especificar una conexión existente como conexión de transporte. Puede especificar una conexión de VPC o una conexión de Direct Connect como conexión de transporte.

Para crear una conexión de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito).
3. Elija Create transit gateway attachment (Crear conexión de gateway de tránsito).
4. (Opcional) En Name tag (Etiqueta de nombre), indique un nombre de etiqueta para la conexión.
5. En Transit Gateway ID (ID de gateway de tránsito), elija la gateway de tránsito para la conexión.
6. En Attachment type (Tipo de conexión), elija Connect.
7. En Transport attachment ID (ID de conexión de transporte), elija el ID de una conexión existente (la conexión de transporte).
8. Elija Create transit gateway attachment (Crear conexión de gateway de tránsito).

Para crear una conexión de Connect mediante la AWS CLI

Utilice el comando create-transit-gateway-connect.

Creación de un emparejamiento en AWS Transit Gateway

Puede crear un par de Connect (túnel de GRE) para una conexión de Connect existente. Antes de comenzar, asegúrese de haber configurado un bloque CIDR de gateway de tránsito. Puede configurar un bloque CIDR de gateway de tránsito cuando crea o modifica una gateway de tránsito.

Cuando crea el par de Connect, debe especificar la dirección IP externa de GRE en el lado del dispositivo del par de Connect.

Para crear un par de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito).
3. Seleccione la conexión de Connect y elija Actions (Acciones), Create Connect peer (Crear par de Connect).
4. (Opcional) En Name tag (Etiqueta de nombre), indique una etiqueta de nombre para la interconexión de Connect.
5. (Opcional) En Transit gateway GRE Address (Dirección de GRE de la gateway de tránsito), especifique la dirección IP externa de GRE para la gateway de tránsito. De forma predeterminada, se utiliza la primera dirección disponible del bloque CIDR de la gateway de tránsito.
6. En Peer GRE Address (Dirección de GRE de la interconexión), especifique la dirección IP externa de GRE para el lado del dispositivo de la interconexión de Connect.
7. En BGP Inside CIDR blocks IPv4 (Bloques CIDR internos IPv4 de BGP), especifique el rango de direcciones IPv4 internas que se utilizan para los pares de BGP. Especifique un bloque CIDR /29 del rango `169.254.0.0/16`.
8. (Optional) En BGP Inside CIDR blocks IPv6 (Bloques CIDR internos IPv6 de BGP), especifique el rango de direcciones IPv6 internas que se utilizan para los pares de BGP. Especifique un bloque CIDR /125 del rango `fd00::/8`.
9. (Opcional) En Peer ASN (ASN del par), especifique el número de sistema autónomo (ASN) para protocolo de gateway fronteriza (BGP) para el dispositivo. Puede utilizar un ASN existente asignado a su red. Si no tiene ninguno, puede utilizar un ASN privado en el rango 64512—65534 (ASN de 16 bits) o en el rango de 4200000000—4294967294 (ASN de 32 bits).

El valor predeterminado es el mismo ASN que la gateway de tránsito. Si configura el ASN del par para que sea diferente al ASN de gateway de tránsito (eBGP), debe configurar ebgp-multihop con un valor de tiempo de vida (TTL) de 2.

10. Elija Create Connect peer (Crear par de Connect).

Para crear una interconexión Connect mediante la AWS CLI

Utilice el comando create-transit-gateway-connect-peer.

Vea los archivos adjuntos de Connect y los compañeros de Connect en AWS Transit Gateway

Consulte las conexiones y los pares de Connect.

Para ver las conexiones y los pares de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito).
3. Seleccione la conexión de Connect.
4. Para ver los pares de Connect para la conexión, elija la pestaña Connect Peers (Pares de Connect).

Para ver sus archivos adjuntos de Connect y sus compañeros de Connect mediante el AWS CLI

Utilice los comandos describe-transit-gateway-connectsy describe-transit-gateway-connect-peers.

Modifique el archivo adjunto Connect y las etiquetas de pares Connect en AWS Transit Gateway

Puede modificar las etiquetas de la conexión de Connect.

Para modificar las etiquetas de la conexión de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Conexiones de gateway de tránsito).

3. Seleccione la conexión de Connect, y luego elija Actions (Acciones), Manage tags (Administrar etiquetas).
4. Para agregar una etiqueta, elija Add new tag (Agregar nueva etiqueta) y especifique el nombre y el valor de la clave.
5. Para eliminar una etiqueta, elija Eliminar.
6. Seleccione Save.

Puede modificar las etiquetas del par de Connect.

Para modificar las etiquetas del par de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateways Attachments (Conexiones de gateway de tránsito).
3. Seleccione la conexión de Connect, y luego elija Connect peers (Pares de Connect).
4. Seleccione la interconexión de Connect y luego elija Actions (Acciones), Manage tags (Administrar etiquetas).
5. Para agregar una etiqueta, elija Add new tag (Agregar nueva etiqueta) y especifique el nombre y el valor de la clave.
6. Para eliminar una etiqueta, elija Eliminar.
7. Seleccione Save.

Para modificar el archivo adjunto de Connect y las etiquetas homólogas de Connect mediante el AWS CLI

Utilice los comandos create-tags y delete-tags.

Eliminar un emparejamiento en AWS Transit Gateway

Si ya no necesita un par de Connect, puede eliminarlo.

Para eliminar un par de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito).

3. Seleccione la conexión de Connect.
4. En la pestaña Connect Peers (Interconexiones de Connect), seleccione la interconexión de Connect y elija Actions (Acciones), Delete Connect peer (Eliminar interconexión de Connect).

Para eliminar una interconexión de Connect mediante la AWS CLI

Utilice el comando delete-transit-gateway-connect-peer.

Eliminar una conexión de Connect en AWS Transit Gateway

Si ya no necesita una conexión de Connect, puede eliminarla. Primero debe eliminar cualquier par de Connect para la conexión.

Para eliminar una conexión de Connect mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit gateway attachments (Conexiones de puerta de enlace de tránsito).
3. Seleccione la conexión de Connect y elijaActions(Acciones), Delete transit gateway attachment (Eliminar conexión de gateway de tránsito).
4. Ingrese **`delete`** y elija Delete (Eliminar).

Para eliminar una conexión de Connect mediante la AWS CLI

Utilice el comando delete-transit-gateway-connect.

Tablas de rutas de Transit Gateway en AWS Transit Gateway

Utilice tablas de enrutamiento de puerta de enlace de tránsito para configurar el enrutamiento para la puerta de enlaces de tránsito. Una tabla de enrutamiento es una tabla que contiene reglas que determinan cómo se enruta el tráfico de la red entre las VPC y las VPN. Cada ruta de la tabla contiene el rango de direcciones IP de los destinos a los que desea enviar el tráfico.

Las tablas de enrutamiento de la puerta de enlace de tránsito permiten asociar una tabla con una conexión de puerta de enlace de tránsito. Se admiten VPC, VPN, VPN Concentrator, Client VPN, Direct Connect Gateway, Peering y Connect adjuntos. Cuando están asociadas, las rutas de estas

conexiones se propagan desde la conexión hacia la tabla de enrutamiento de la puerta de enlace de tránsito de destino. Una conexión se puede propagar a varias tablas de enrutamiento.

Además, puede crear y administrar rutas estáticas con una tabla de enrutamiento. Por ejemplo, es posible que tenga una ruta estática que se utilice como ruta de respaldo en caso de que se produzca una interrupción de la red que afecte a cualquier ruta dinámica.

Tareas

- Crear una tabla de enrutamiento de la puerta de enlace de tránsito en AWS Transit Gateway
- Vea las tablas de rutas de Transit Gateway con AWS Transit Gateway
- Asociar una tabla de enrutamiento de la puerta de enlace de tránsito en AWS Transit Gateway
- Eliminar una asociación para una tabla de rutas de Transit Gateway en AWS Transit Gateway
- Habilitar la propagación de rutas a una tabla de rutas de Transit Gateway en AWS Transit Gateway
- Deshabilitación de la propagación de rutas con AWS Transit Gateway
- Crear una ruta estática en AWS Transit Gateway
- Eliminar una ruta estática en AWS Transit Gateway
- Reemplazar una ruta estática en AWS Transit Gateway
- Exportar tablas de enrutamiento a Amazon S3 en AWS Transit Gateway
- Eliminar una tabla de enrutamiento de la puerta de enlace de tránsito en AWS Transit Gateway
- Crear una referencia de lista de prefijos para la tabla de enrutamiento en AWS Transit Gateway
- Modificar una referencia de lista de prefijos en AWS Transit Gateway
- Eliminar una referencia de lista de prefijos en AWS Transit Gateway

Crear una tabla de enrutamiento de la puerta de enlace de tránsito en AWS Transit Gateway

Para crear una tabla de enrutamiento de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Elija Create transit gateway route table (Crear tabla de enrutamiento de puerta de enlace de tránsito).

4. (Opcional) En Name tag (Etiqueta de nombre), escriba un nombre para la tabla de enrutamiento de la puerta de enlace de tránsito. Al hacerlo, se crea una etiqueta con la clave de etiqueta "Name (Nombre)", en la que el valor de la etiqueta es el nombre que especifique.
5. En Transit gateway ID (ID de puerta de enlace de tránsito), seleccione la puerta de enlace de tránsito de la tabla de enrutamiento.
6. Elija Create transit puerta de enlace route table (Crear tabla de enrutamiento de puerta de enlace de tránsito).

Para crear una tabla de enrutamiento de puerta de enlace de tránsito mediante AWS CLI

Utilice el comando create-transit-gateway-route-table.

Vea las tablas de rutas de Transit Gateway con AWS Transit Gateway

Para consultar las tablas de enrutamiento de la puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. (Opcional) Para encontrar una tabla de enrutamiento o un conjunto de tablas en especial, escriba la totalidad o parte del nombre, de la palabra clave o del atributo en el campo de filtro.
4. Active la casilla de verificación de una tabla de enrutamiento o elija su ID para mostrar información sobre sus asociaciones, propagaciones, rutas y etiquetas.

Para ver las tablas de rutas de tu pasarela de transporte público utilizando el AWS CLI

Usa el comando describe-transit-gateway-route-tables.

Para ver las rutas de una tabla de rutas de una puerta de enlace de tránsito mediante el AWS CLI

Utilice el comando search-transit-gateway-routes.

Para ver las propagaciones de rutas de una tabla de rutas de una puerta de enlace de tránsito mediante el AWS CLI

Utilice el comando get-transit-gateway-route-table-propagations.

Para ver las asociaciones de una tabla de rutas de una puerta de enlace de tránsito mediante el AWS CLI

Utilice el comando get-transit-gateway-route-table-associations.

Asociar una tabla de enrutamiento de la puerta de enlace de tránsito en AWS Transit Gateway

Puede asociar una tabla de enrutamiento de puerta de enlace de tránsito con una puerta de enlaces de tránsito.

Para asociar una tabla de enrutamiento de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento.
4. En la parte inferior de la página, elija la pestaña Associations (Asociaciones).
5. Elija Create association (Crear asociación).
6. Elija la vinculación que se va a asociar y, a continuación, elija Create association (Crear asociación).

Para asociar una tabla de enrutamiento de puerta de enlace de tránsito mediante AWS CLI

Utilice el comando associate-transit-gateway-route-table.

Eliminar una asociación para una tabla de rutas de Transit Gateway en AWS Transit Gateway

Puede desasociar una tabla de enrutamiento de puerta de enlace de tránsito de una puerta de enlaces de tránsito.

Para desasociar una tabla de enrutamiento de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento.
4. En la parte inferior de la página, elija la pestaña Associations (Asociaciones).

5. Elija la vinculación que desea desasociar y, a continuación, elija Delete association (Eliminar asociación).
6. Cuando se le pida que confirme, elija Delete association (Eliminar asociación).

Para desasociar una tabla de rutas de una pasarela de tránsito mediante el AWS CLI

Utilice el comando disassociate-transit-gateway-route-table.

Habilitar la propagación de rutas a una tabla de rutas de Transit Gateway en AWS Transit Gateway

Utilice la propagación de rutas para agregar una ruta de una vinculación a una tabla de enrutamiento.

Para propagar una ruta a una tabla de enrutamiento de puerta de enlaces de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento para la que se va a crear una propagación.
4. Elija Actions (Acciones) y, después, Create propagation (Crear propagación).
5. En la página Create propagation (Crear propagación), elija la vinculación.
6. Elija Create propagation (Crear propagación).

Para habilitar la propagación de rutas mediante el AWS CLI

Utilice el comando enable-transit-gateway-route-table-propagation.

Deshabilitación de la propagación de rutas con AWS Transit Gateway

Quite una ruta propagada de una vinculación de tabla de enrutamiento.

Para deshabilitar la propagación de rutas utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).

3. Seleccione la tabla de enrutamiento de la que desea eliminar la propagación.
4. En la parte inferior de la página, elija la pestaña Propagations (Propagaciones).
5. Seleccione la vinculación y, a continuación, elija Delete propagation (Eliminar propagación).
6. Cuando se le pida que confirme, elija Delete propagation (Eliminar propagación).

Para deshabilitar la propagación de rutas mediante la AWS CLI

Utilice el comando disable-transit-gateway-route-table-propagation.

Crear una ruta estática en AWS Transit Gateway

Cree una ruta estática para una VPC, VPN o vinculación de interconexión de puerta de enlace de tránsito, o puede crear una ruta de agujero negro que borre el tráfico que llegue a la ruta.

Las rutas estáticas de una tabla de enrutamiento de puerta de enlace de tránsito que se dirigen a una conexión de VPN no son filtradas por la Site-to-Site VPN. Esto podría permitir el flujo de tráfico saliente no deseado cuando se utiliza una VPN basada en BGP.

Para crear una ruta estática utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento para la que se va a crear una ruta.
4. Elija Actions (Acciones), Create static route (Crear ruta estática).
5. En la página Create static route (Crear ruta estática), ingrese el bloque de CIDR para el que se debe crear la ruta, y luego elija Active (Activo).
6. Seleccione la vinculación para la ruta.
7. Elija Create static route (Crear ruta estática).

Para crear una ruta de agujero negro utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).

3. Seleccione la tabla de enrutamiento para la que se va a crear una ruta.
4. Elija Actions (Acciones), Create static route (Crear ruta estática).
5. En la página Create static route (Crear ruta estática), ingrese el bloque de CIDR para el que se debe crear la ruta, y luego elija Blackhole (Agujero negro).
6. Elija Create static route (Crear ruta estática).

Para crear una ruta estática o una ruta de agujero negro utilizando la AWS CLI

Utilice el comando create-transit-gateway-route.

Eliminar una ruta estática en AWS Transit Gateway

Elimine las rutas estáticas de una tabla de enrutamiento de la puerta de enlace de tránsito.

Para eliminar una ruta estática utilizando la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento para la que desea eliminar la ruta y, a continuación, elija Routes (Rutas).
4. Elija la ruta que se va a eliminar.
5. Elija Delete static route (Eliminar ruta estática).
6. En el cuadro de confirmación, elija Delete static route (Eliminar ruta estática).

Para eliminar una ruta estática utilizando la AWS CLI

Utilice el comando delete-transit-gateway-route.

Reemplazar una ruta estática en AWS Transit Gateway

Reemplace una ruta estática en la tabla de enrutamiento de una puerta de enlace por una ruta estática diferente.

Para reemplazar una ruta estática utilizando la consola

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

2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Elija la ruta que desee reemplazar en la tabla de enrutamiento.
4. En la sección de detalles, seleccione la pestaña Rutas.
5. Elija Acciones, Reemplazar ruta estática.
6. Para el Tipo, elija Activo o Agujero negro.
7. En el menú desplegable Elegir archivo adjunto, elija la puerta de enlace que sustituirá a la actual en la tabla de enrutamiento.
8. Elija Reemplazar ruta estática.

Para reemplazar una ruta estática mediante la AWS CLI

Utilice el comando replace-transit-gateway-route.

Exportar tablas de enrutamiento a Amazon S3 en AWS Transit Gateway

Puede exportar las rutas de las tablas de enrutamiento de la puerta de enlace de tránsito a un bucket de Amazon S3. Las rutas se guardan en un archivo JSON que se almacena en el bucket de Amazon S3 especificado.

Para exportar tablas de enrutamiento de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Elija la tabla de enrutamiento que incluye las rutas que va a exportar.
4. Elija Actions (Acciones), Export routes (Exportar rutas).
5. En la página Export routes (Exportar rutas), escriba el nombre del bucket de S3 en S3 bucket name (Nombre del bucket de S3).
6. Para filtrar las rutas exportadas, especifique los parámetros de filtrado en la sección Filters (Filtros) de la página.
7. Elija Export routes (Exportar rutas).

Para acceder a las rutas exportadas, abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/ y vaya al bucket especificado. El nombre del archivo incluye el ID

de Cuenta de AWS, la región de AWS, el ID de la tabla de enrutamiento y una marca temporal. Seleccione el archivo y elija Download (Descargar). A continuación, se muestra un ejemplo de un archivo JSON que contiene información sobre dos rutas de adjuntos de la VPC propagadas.


```
{
  "filter": [
    {
      "name": "route-search.subnet-of-match",
      "values": [
        "0.0.0.0/0",
        "::/0"
      ]
    }
  ],
  "routes": [
    {
      "destinationCidrBlock": "10.0.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-0123456abcd123456",
          "transitGatewayAttachmentId": "tgw-attach-1122334455aabbcc1",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    },
    {
      "destinationCidrBlock": "10.2.0.0/16",
      "transitGatewayAttachments": [
        {
          "resourceId": "vpc-abcabc123123abca",
          "transitGatewayAttachmentId": "tgw-attach-6677889900aabbcc7",
          "resourceType": "vpc"
        }
      ],
      "type": "propagated",
      "state": "active"
    }
  ]
}
```

Eliminar una tabla de enrutamiento de la puerta de enlace de tránsito en AWS Transit Gateway

Para eliminar una tabla de enrutamiento de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Seleccione la tabla de enrutamiento que desea eliminar.
4. Elija Actions (Acciones), Delete transit gateway route table (Eliminar tabla de enrutamiento de puerta de enlace de tránsito).
5. Ingrese **`delete`** y elija Delete (Eliminar) para confirmar la eliminación.

Para eliminar una tabla de enrutamiento de puerta de enlace de tránsito mediante AWS CLI

Utilice el comando delete-transit-puerta de enlace-route-table.

Crear una referencia de lista de prefijos para la tabla de enrutamiento en AWS Transit Gateway

Puede hacer referencia a una lista de prefijos en la tabla de enrutamiento de la gateway de tránsito. Una lista de prefijos es un conjunto de una o más entradas de bloque de CIDR que se definen y administran. Puede utilizar una lista de prefijos para simplificar la administración de las direcciones IP a las que hace referencia en los recursos para enrutar el tráfico de red. Por ejemplo, si especifica con frecuencia los mismos CIDR de destino en varias tablas de enrutamiento de gateway de tránsito, puede administrar esos CIDR en una sola lista de prefijos, en lugar de hacer repetidas referencias a los mismos CIDR en cada tabla de enrutamiento. Si necesita quitar un bloque de CIDR de destino, puede eliminar su entrada de la lista de prefijos en lugar de eliminar la ruta de todas las tablas de enrutamiento afectadas.

Al crear una referencia de lista de prefijos en la tabla de enrutamiento de la gateway de tránsito, cada entrada de la lista de prefijos se representa como una ruta en la tabla de enrutamiento de la gateway de tránsito.

Para obtener más información sobre las listas de prefijos, consulte Listas de prefijos en la Guía del usuario de Amazon VPC.

Para crear una referencia de lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de enrutamiento de gateway de tránsito).
3. Seleccione la tabla de enrutamiento de la gateway de tránsito.
4. Elija Actions (Acciones), Create prefix list reference (Crear referencia de lista de prefijos).
5. Para Prefix list ID (ID de lista de prefijos), elija el ID de lista de prefijos.
6. En Type (Tipo), elija si el tráfico dirigido a esta lista de prefijos se debe permitir (Active (Activo)) o descartar (Blackhole (Agujero negro)).
7. En Transit gateway attachment ID (ID de conexión de gateway de tránsito), elija el ID de la conexión a la que se debe dirigir el tráfico.
8. Elija Create prefix list reference (Crear referencia de lista de prefijos).

Para crear una referencia de lista de prefijos mediante la AWS CLI (AWS CLI)

Utilice el comando create-transit-gateway-prefix-list-reference.

Modificar una referencia de lista de prefijos en AWS Transit Gateway

Puede modificar una referencia de lista de prefijos cambiando la vinculación a la que se dirige el tráfico o indicando si desea eliminar el tráfico que coincide con la ruta.

No se pueden modificar las rutas individuales de una lista de prefijos en la pestaña Routes (Rutas). Para modificar las entradas de la lista de prefijos, utilice la pantalla Managed Prefix Lists (Listas de prefijos administradas). Para obtener más información, consulte Modificación de una lista de prefijos en la Guía del usuario de Amazon VPC.

Para modificar una referencia de lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de enrutamiento de gateway de tránsito).
3. Seleccione la tabla de enrutamiento de la gateway de tránsito.
4. En el panel inferior, elija Prefix list references (Referencias de lista de prefijos).
5. Elija la referencia de la lista de prefijos, y luego Modify references (Modificar referencias).

6. En Type (Tipo), elija si el tráfico dirigido a esta lista de prefijos se debe permitir (Active (Activo)) o descartar (Blackhole (Agujero negro)).
7. En Transit gateway attachment ID (ID de conexión de gateway de tránsito), elija el ID de la conexión a la que se debe dirigir el tráfico.
8. Elija Modify prefix list reference (Modificar referencia de lista de prefijos).

Para modificar una referencia de lista de prefijos mediante la AWS CLI (AWS CLI)

Utilice el comando modify-transit-gateway-prefix-list-reference.

Eliminar una referencia de lista de prefijos en AWS Transit Gateway

Si ya no necesita una referencia de lista de prefijos, puede eliminarla de la tabla de enrutamiento de la gateway de tránsito. La eliminación de la referencia no elimina la lista de prefijos.

Para eliminar una referencia de lista de prefijos mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de enrutamiento de gateway de tránsito).
3. Seleccione la tabla de enrutamiento de la gateway de tránsito.
4. Elija la referencia de la lista de prefijos, y luego Delete references (Eliminar referencias).
5. Elija Delete references (Eliminar referencias).

Para modificar una referencia de lista de prefijos mediante la AWS CLI (AWS CLI)

Utilice el comando delete-transit-gateway-prefix-list-reference.

Tablas de políticas de la puerta de enlace de tránsito en AWS Transit Gateway

El enrutamiento dinámico de puerta de enlace de tránsito utiliza tablas de políticas para enrutar el tráfico de red para AWS Cloud WAN. La tabla contiene reglas de políticas para hacer coincidir el tráfico de red por atributos de política y, a continuación, asigna el tráfico que coincide con la regla a una tabla de enrutamiento de destino.

Puede utilizar el enrutamiento dinámico para puertas de enlace de tránsito para intercambiar automáticamente información de enrutamiento y accesibilidad con tipos de puertas de enlace de tránsito interconectadas. A diferencia de una ruta estática, el tráfico se puede enrutar a lo largo de una ruta diferente según las condiciones de la red, como fallas de ruta o congestión. El enrutamiento dinámico también agrega una capa adicional de seguridad, ya que es más fácil redirigir el tráfico en caso de una violación o incursión en la red.

> **Note**
>
> Las tablas de políticas de puerta de enlace de tránsito actualmente solo se admiten en Cloud WAN al crear una vinculación de interconexión de la puerta de enlace de tránsito. Al crear una vinculación de interconexión, puede asociar esa tabla a la conexión. A continuación, la asociación rellena la tabla automáticamente con las reglas de la política.
> Para obtener más información sobre Cloud WAN, consulte Peerings (Interconexiones) en la Guía del usuario de Cloud WAN de AWS.

Tareas

- Cree una tabla de políticas de Transit Gateway en AWS Transit Gateway
- Eliminar una tabla de políticas de Transit Gateway en AWS Transit Gateway

Cree una tabla de políticas de Transit Gateway en AWS Transit Gateway

Para crear una tabla de política de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Table (Tabla de enrutamiento de puerta de enlace de tránsito).
3. Elija Create transit puerta de enlace route table (Crear tabla de políticas de puerta de enlace de tránsito).
4. (Opcional) En Name tag (Etiqueta de nombre), ingrese un nombre para la tabla de políticas de puerta de enlace de tránsito. Esto crea una etiqueta, donde el valor de la etiqueta es el nombre que usted especifique.
5. Para el ID de puerta de enlace de tránsito, seleccione la puerta de enlace de tránsito de la tabla de enrutamiento.

6. Elija Create transit puerta de enlace route table (Crear tabla de políticas de puerta de enlace de tránsito).

Para crear una tabla de políticas de pasarelas de tránsito mediante el AWS CLI

Utilice el comando create-transit-gateway-policy-table.

Eliminar una tabla de políticas de Transit Gateway en AWS Transit Gateway

Elimine una tabla de enrutamiento de la puerta de enlace de tránsito. Cuando se elimina una tabla, se eliminan todas las reglas de política de esa tabla.

Para eliminar una tabla de política de puerta de enlace de tránsito mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway Route Tables (Tablas de ruteo de puerta de enlace de tránsito).
3. Elija la tabla de políticas de puerta de enlace de tránsito que desea eliminar.
4. Seleccione Actions (Acciones) y Delete policy table (Eliminar tabla de políticas).
5. Confirme que desea eliminar la tabla.

Para eliminar una tabla de políticas de pasarelas de tránsito mediante el AWS CLI

Utilice el comando delete-transit-gateway-policy-table.

Multidifusión en AWS Transit Gateway

La multidifusión es un protocolo de comunicación empleado para el envío de un solo flujo de datos a varios equipos receptores de forma simultánea Transit Gateway admite el enrutamiento del tráfico de multidifusión entre subredes de VPC asociadas y sirve como enrutador de multidifusión para instancias que envían tráfico destinado a varias instancias receptoras.

Temas

- Conceptos de la multidifusión
- Consideraciones

- Enrutar multidifusión
- Dominios de multidifusión en AWS Transit Gateway
- Dominios de multidifusión compartidos en AWS Transit Gateway
- Registrar fuentes con un grupo de multidifusión en AWS Transit Gateway
- Registrar miembros con un grupo de multidifusión en AWS Transit Gateway
- Anulación del registro de orígenes del grupo de multidifusión de AWS Transit Gateway
- Anular el registro de miembros de un grupo de multidifusión en Transit Gateway AWS
- Ver grupos de multidifusión en AWS Transit Gateway
- Configuración de la multidifusión para Windows Server en AWS Transit Gateway
- Ejemplo: administrar las configuraciones IGMP mediante AWS Transit Gateway
- Ejemplo: administrar configuraciones de fuentes estáticas en AWS Transit Gateway
- Ejemplo: administrar las configuraciones estáticas de los miembros de un grupo en AWS Transit Gateway

Conceptos de la multidifusión

A continuación se enumeran los conceptos clave de la multidifusión:

- Dominio de multidifusión: permite la segmentación de una red de multidifusión en distintos dominios y hace que la puerta de enlace de tránsito actúe como varios enrutadores de multidifusión. Defina la pertenencia al dominio de multidifusión en el nivel de subred.
- Grupo de multidifusión: identifica un conjunto de hosts que enviarán y recibirán el mismo tráfico de multidifusión. Un grupo de multidifusión se identifica por una dirección IP de grupo. La pertenencia a un grupo de multidifusión se define como una interfaz de red elástica asociada a instancias EC2
- Protocolo de administración de grupos de Internet (IGMP): protocolo de Internet que permite a los hosts y enrutadores administrar dinámicamente la pertenencia a grupos de multidifusión. Un dominio de multidifusión IGMP contiene hosts que utilizan el protocolo IGMP para unirse, salir y enviar mensajes. AWS admite el protocolo IGMPv2 y dominios de multidifusión de pertenencia a grupos estáticos (basados en API) y IGMP.

- Origen de multidifusión: interfaz de red elástica asociada a una instancia EC2 compatible que está configurada estáticamente para enviar tráfico de multidifusión. Un origen de multidifusión solo se aplica a las configuraciones de origen estático.

Un dominio de multidifusión de origen estático contiene hosts que no utilizan el protocolo IGMP para unirse, salir y enviar mensajes. Utilice la AWS CLI para agregar un origen y miembros de grupo. El origen agregado estáticamente envía tráfico de multidifusión y los miembros reciben tráfico de multidifusión.

- Miembro de grupo de multidifusión: una interfaz de red elástica asociada con una instancia EC2 compatible que recibe tráfico de multidifusión. Un grupo de multidifusión cuenta con varios miembros en el grupo. En una configuración de pertenencia a un grupo de origen estático, los miembros del grupo de multidifusión solo pueden recibir tráfico. En una configuración de grupo de IGMP, los miembros pueden enviar y recibir tráfico.

Consideraciones

- La multidifusión de la puerta de enlace puede no ser adecuada para operaciones de alta frecuencia o aplicaciones sensibles al rendimiento. Le aconsejamos encarecidamente que revise las cuotas de multidifusión para conocer los límites. Póngase en contacto con el equipo de su cuenta o de arquitectos de soluciones para obtener una revisión detallada de sus requisitos de rendimiento.
- Para obtener información acerca de las regiones admitidas, consulte las Preguntas frecuentes de AWS Transit Gateway.
- Debe crear una nueva puerta de enlace de tránsito para admitir la multidifusión.
- La pertenencia a un grupo de multidifusión se administra mediante el uso de la Amazon Virtual Private Cloud Console, la AWS CLI o el IGMP.
- Una subred solo puede estar en un dominio de multidifusión.
- Si utiliza una instancia que no sea Nitro, debe desmarcar la casilla de verificación Origen/Destino. Para obtener información sobre cómo desactivar la comprobación, consulte Cambio de comprobación de origen o destino en la Guía del usuario de Amazon EC2.
- Una instancia que no sea Nitro no puede ser remitente de multidifusión.
- El enrutamiento de multidifusión no se admite a través de Direct Connect, VPN de sitio a sitio, vinculaciones de interconexiones o vinculaciones de Transit Gateway Connect.
- Una puerta de enlace de tránsito no admite la fragmentación de paquetes de multidifusión. Los paquetes de multidifusión fragmentados se eliminan. Para obtener más información, consulte Unidad de transmisión máxima (MTU)..

- Cuando se inicia, un host de IGMP envía varios mensajes de IGMP JOIN para unirse a un grupo de multidifusión (normalmente de 2 a 3 reintentos). En el caso improbable de que se pierdan todos los mensajes de IGMP JOIN, el host no pasará a formar parte del grupo de multidifusión de puerta de enlace de tránsito. En tal escenario, deberá volver a activar el mensaje de IGMP JOIN desde el host mediante métodos específicos de la aplicación.
- La pertenencia a un grupo comienza con la recepción del mensaje JOIN de IGMPv2 por parte de la puerta de enlace de tránsito y finaliza con la recepción del mensaje LEAVE de IGMPv2. La puerta de enlace de tránsito realiza un seguimiento de los hosts que se unieron correctamente al grupo. Como enrutador de multidifusión en la nube, la puerta de enlace de tránsito emite un mensaje QUERY de IGMPv2 a todos los miembros cada dos minutos. Cada miembro envía un mensaje JOIN de IGMPv2 como respuesta, que es la forma en que los miembros renuevan su pertenencia. Si un miembro no responde a tres consultas consecutivas, la puerta de enlace de tránsito elimina esta pertenencia de todos los grupos a los que se unió. Sin embargo, continúa enviando consultas a este miembro durante 12 horas antes de eliminarlo permanentemente de la lista a consultar. Un mensaje LEAVE explícito de IGMPv2 elimina de forma inmediata y permanente el host de cualquier otro procesamiento de multidifusión.
- La puerta de enlace de tránsito realiza un seguimiento de los hosts que se unieron correctamente al grupo. En caso de interrupción de la puerta de enlace de tránsito, esta continúa enviando datos de multidifusión al host durante siete minutos (420 segundos) después del último mensaje JOIN de IGMP correcto. La puerta de enlace de tránsito continúa enviando consultas de pertenencia al host durante un máximo de 12 horas o hasta que reciba un mensaje IGMP LEAVE del host.
- La puerta de enlace de tránsito envía paquetes de consulta de pertenencia a todos los miembros de IGMP para que pueda realizar un seguimiento de la pertenencia a grupos de multidifusión. La IP de origen de estos paquetes de consulta de IGMP es 0.0.0.0/32 y la IP de destino es 224.0.0.1/32 y el protocolo es 2. La configuración del grupo de seguridad en los host de IGMP (instancias) y cualquier configuración de ACL en las subredes de host deben permitir estos mensajes de protocolo IGMP.
- Cuando la fuente y el destino de multidifusión se encuentran en la misma VPC, no se puede utilizar la referencia del grupo de seguridad para establecer el grupo de seguridad de destino con objeto de aceptar tráfico procedente del grupo de seguridad de la fuente.
- En el caso de los grupos y fuentes de multidifusión estáticos, AWS Transit Gateway elimina automáticamente los grupos y fuentes estáticos de las ENI que ya no existen. Esto se realiza asumiendo periódicamente la función de enlace al servicio Transit Gateway para describir los ENI de la cuenta.
- Solo la multidifusión estática es compatible con IPv6. La multidifusión dinámica no lo es.

Enrutar multidifusión

Cuando habilita la multidifusión en una gateway de tránsito, actúa como enrutador de multidifusión. Cuando agrega una subred a un dominio de multidifusión, enviamos todo el tráfico de multidifusión a la gateway de tránsito que se asocia con un dominio de multidifusión.

ACL de red

Las reglas de ACL de red funcionan en el nivel de subred. Se aplican al tráfico de multidifusión, ya que las puertas de enlace de tránsito residen fuera de la subred. Para obtener más información, consulte ACL de puntos de enlace en la Guía del usuario de Amazon VPC.

Para el tráfico de multidifusión de Protocolo de administración de grupo de Internet (IGMP), las siguientes son las reglas de entrada mínimas. El host remoto es el host que envía el tráfico de multidifusión.

Tipo	Protocolo	Fuente	Descripción
Protocolo personalizado	IGMP(2)	0.0.0.0/32	Consulta de IGMP
Protocolo UDP personalizado	UDP	Dirección IP del host remoto	Tráfico de multidifusión entrante

Las siguientes son las reglas mínimas de salida para IGMP.

Tipo	Protocolo	Destino	Descripción
Protocolo personalizado	IGMP(2)	224.0.0.2/32	Ausencia de IGMP
Protocolo personalizado	IGMP(2)	Dirección IP del grupo de multidifusión	Combinación de IGMP
Protocolo UDP personalizado	UDP	Dirección IP del grupo de multidifusión	Tráfico de multidifusión saliente

Grupos de seguridad

Las reglas de grupos de seguridad funcionan en el nivel de la instancia. Se pueden aplicar al tráfico de multidifusión entrante y saliente. El comportamiento es igual que en el tráfico de unidifusión. Para todos las instancias de miembros del grupo, debe permitir el tráfico saliente desde la fuente del grupo. Para obtener más información, consulte Grupo de seguridad en la Guía del usuario de Amazon VPC.

Debe tener las siguientes reglas de entrada como mínimo para el tráfico de multidifusión de IGMP. El host remoto es el host que envía el tráfico de multidifusión. No se puede especificar un grupo de seguridad como origen de la regla de entrada UDP.

Tipo	Protocolo	Fuente	Descripción
Protocolo personalizado	2	0.0.0.0/32	Consulta de IGMP
Protocolo UDP personalizado	UDP	Dirección IP del host remoto	Tráfico de multidifusión entrante

Debe tener las siguientes reglas de salida como mínimo para el tráfico de multidifusión de IGMP.

Tipo	Protocolo	Destino	Descripción
Protocolo personalizado	2	224.0.0.2/32	Ausencia de IGMP
Protocolo personalizado	2	Dirección IP del grupo de multidifusión	Combinación de IGMP
Protocolo UDP personalizado	UDP	Dirección IP del grupo de multidifusión	Tráfico de multidifusión saliente

Dominios de multidifusión en AWS Transit Gateway

Un dominio de multidifusión permite la segmentación de una red de multidifusión en distintos dominios. Para comenzar a utilizar la multidifusión con una gateway de tránsito, cree un dominio de multidifusión y, a continuación, asocie subredes con el dominio.

Atributos de dominio de multidifusión

En la siguiente tabla se detallan los atributos de dominio de multidifusión. No se pueden habilitar ambos atributos al mismo tiempo.

Atributo	Descripción
`Igmpv2Support` (AWS CLI) IGMPv2 support (Compatibilidad con IGMPv2) (consola)	Este atributo determina cómo los miembros del grupo se unen o abandonan un grupo de multidifusión. Cuando este atributo está desactivado, se deben agregar manualmente los miembros del grupo al dominio. Habilite este atributo si al menos un miembro utiliza el protocolo IGMP. Los miembros se unen al grupo de multidifusión de una de las siguientes maneras: • Los miembros que admiten IGMP utilizan los mensajes `JOIN` y `LEAVE`. • Los miembros que no admiten IGMP deben agregarse o eliminarse del grupo mediante la consola de Amazon VPC o la AWS CLI. Si registra miembros del grupo de multidifusión, también debe anular su registro. La puerta de enlace de tránsito ignora un mensaje de IGMP `LEAVE` enviado por un miembro del grupo agregado manualmente.
`StaticSourcesSupport` (AWS CLI) Static sources support (Compatibilidad con fuentes estáticas) (consola)	Este atributo determina si hay orígenes de multidifusión estáticos para el grupo. Cuando este atributo está activado, se deben agregar las fuentes de un dominio de multidifusión mediante register-transit-gateway-multicast-group-sources. Solo los orígenes de multidifusión pueden enviar tráfico de multidifusión. Cuando este atributo está deshabilitado, no hay fuentes de multidifusión designadas. Cualquier instancia que se encuentre

Atributo	Descripción
	en subredes asociadas al dominio de multidifusión puede enviar tráfico de multidifusión y los miembros del grupo reciben el tráfico de multidifusión.

Cree un dominio de multidifusión IGMP en AWS Transit Gateway

Si aún no lo ha hecho, revise los atributos de dominio de multidifusión disponibles. Para obtener más información, consulte the section called “Dominios de multidifusión”.

Para crear un dominio de multidifusión de IGMP mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Elija Create transit gateway multicast domain (Crear dominio de multidifusión de puerta de enlace de tránsito).
4. En Name tag (Etiqueta de nombre), ingrese un nombre para el dominio.
5. En Transit gateway ID (ID de puerta de enlace de tránsito), elija la gateway de tránsito que procesa el tráfico de multidifusión.
6. Para obtener IGMPv2 asistencia, selecciona la casilla de verificación.
7. En Compatibilidad con orígenes estáticos, desmarque la casilla de verificación.
8. Para aceptar automáticamente asociaciones de subred entre cuentas para este dominio de multidifusión, seleccione Auto accept shared associations (Aceptar asociaciones compartidas automáticamente).
9. Elija Create transit gateway multicast domain (Crear dominio de multidifusión de gateway de tránsito).

Para crear un dominio de multidifusión IGMP mediante AWS CLI

Utilice el comando create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=disable,Igmpv2Support=enable
```

Creación de un dominio de multidifusión de origen estático con AWS Transit Gateway

Si aún no lo ha hecho, revise los atributos de dominio de multidifusión disponibles. Para obtener más información, consulte the section called “Dominios de multidifusión”.

Para crear un dominio de multidifusión estática mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Elija Create transit gateway multicast domain (Crear dominio de multidifusión de gateway de tránsito).
4. En Name tag (Etiqueta de nombre), escriba un nombre para identificar el dominio.
5. En Transit gateway ID (ID de gateway de tránsito), elija la gateway de tránsito que procesa el tráfico de multidifusión.
6. En Compatibilidad con IGMPv2, desmarque la casilla de verificación.
7. En Compatibilidad con orígenes estáticos, marque la casilla de verificación.
8. Para aceptar automáticamente asociaciones de subred entre cuentas para este dominio de multidifusión, seleccione Auto accept shared associations (Aceptar asociaciones compartidas automáticamente).
9. Elija Create transit gateway multicast domain (Crear dominio de multidifusión de gateway de tránsito).

Para crear un dominio de multidifusión estática mediante la AWS CLI (AWS CLI)

Utilice el comando create-transit-gateway-multicast-domain.

```
aws ec2 create-transit-gateway-multicast-domain --transit-gateway-
id tgw-0xexampleid12345 --options StaticSourcesSupport=enable,Igmpv2Support=disable
```

Asociación de subredes y adjuntos de VPC a un dominio de multidifusión en Transit Gateway AWS

Utilice el siguiente procedimiento para asociar una vinculación de VPC a un dominio de multidifusión. Al crear una asociación, puede seleccionar las subredes para incluirlas en el dominio de multidifusión.

Antes de comenzar, debe crear una vinculación de la VPC en la puerta de enlace de tránsito. Para obtener más información, consulte Archivos adjuntos de Amazon VPC en AWS Transit Gateway.

Para asociar conexiones de VPC a un dominio de multidifusión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Seleccione el dominio de multidifusión y, a continuación, elija Actions (Acciones), Create association (Crear asociación).
4. En Choose attachment to associate (Elegir la conexión que asociar), seleccione la conexión de puerta de enlace de tránsito.
5. En Choose subnets to associate (Seleccionar las subredes que desea asociar), seleccione las subredes para incluirlas en el dominio de multidifusión.
6. Elija Create association (Crear asociación).

Para asociar los adjuntos de la VPC a un dominio de multidifusión mediante AWS CLI

Utilice el comando associate-transit-gateway-multicast-domain.

Disociar una subred de un dominio de multidifusión en AWS Transit Gateway

Utilice el siguiente procedimiento para desasociar subredes de un dominio de multidifusión.

Para desasociar las subredes mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de gateway de tránsito).
3. Seleccione el dominio de multidifusión.
4. Seleccione la pestaña Associations (Asociaciones).
5. Seleccione la subred y luego elija Actions (Acciones), Delete association (Eliminar asociación).

Para desasociar las subredes mediante la AWS CLI

Utilice el comando disassociate-transit-gateway-multicast-domain.

Ver asociaciones de dominios de multidifusión en AWS Transit Gateway

Consulte sus dominios de multidifusión para verificar que estén disponibles y que contengan las subredes y las conexiones apropiadas.

Para visualizar un dominio de multidifusión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Seleccione el dominio de multidifusión.
4. Seleccione la pestaña Associations (Asociaciones).

Para ver un dominio de multidifusión mediante AWS CLI

Utilice el comando describe-transit-gateway-multicast-domains.

Agregar etiquetas a un dominio de multidifusión en AWS Transit Gateway

Agregue etiquetas a sus recursos para organizarlos e identificarlos mejor, por ejemplo, por objetivo, propietario o entorno. Puede agregar varias etiquetas a cada dominio de multidifusión. Las claves de etiqueta deben ser únicas para cada dominio de multidifusión. Si agrega una etiqueta con una clave que ya está asociada al dominio de multidifusión, actualizará el valor de esa etiqueta. Para obtener más información, consulte Etiquetado de los recursos de Amazon EC2.

Para agregar etiquetas a un dominio de multidifusión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de gateway de tránsito).
3. Seleccione el dominio de multidifusión.
4. Elija Actions (Acciones) y, a continuación, Manage tags (Administrar etiquetas).
5. (Opcional) Para cada etiqueta, elija Add new tag (Agregar nueva etiqueta) e ingrese la Key (Clave) y el Value (Valor) de la etiqueta.
6. Seleccione Save (Guardar).

Para agregar etiquetas a un dominio de multidifusión mediante la AWS CLI

Utilice el comando create-tags.

Eliminar un dominio de multidifusión en AWS Transit Gateway

Utilice el siguiente procedimiento para eliminar un dominio de multidifusión.

Para eliminar un dominio de multidifusión mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de gateway de tránsito).
3. Seleccione el dominio de multidifusión y, a continuación, seleccione Actions (Acciones), Delete multicast domain (Eliminar dominio de multidifusión).
4. Cuando se le pida confirmación, ingrese **`delete`** y elija Delete (Eliminar).

Para eliminar un dominio de multidifusión mediante la AWS CLI (AWS CLI)

Utilice el comando delete-transit-gateway-multicast-domain.

Dominios de multidifusión compartidos en AWS Transit Gateway

Con el uso compartido de dominios de multidifusión, los propietarios de dominios de multidifusión pueden compartir el dominio con otras cuentas de AWS dentro de su organización o entre organizaciones en AWS Organizations. Como propietario del dominio de multidifusión, puede crear y administrar el dominio de multidifusión de forma centralizada. Una vez compartidos, esos usuarios pueden realizar las siguientes operaciones en un dominio de multidifusión compartido:

- Registrar y anular el registro de miembros del grupo u orígenes de grupo en el dominio de multidifusión
- Asociar una subred con el dominio de multidifusión y desasociar subredes del dominio de multidifusión

Un propietario de dominio de multidifusión puede compartir un dominio de multidifusión con:

- AWS cuentas dentro de su organización o entre organizaciones en AWS Organizations
- Una unidad organizativa dentro de su organización en AWS Organizations
- Toda su organización en AWS Organizations

- AWS cuentas fuera de AWS Organizations.

  Para compartir un dominio de multidifusión con una AWS cuenta ajena a su organización, debe crear un recurso compartido utilizando y AWS Resource Access Manager, a continuación, elegir Permitir compartir con cualquier persona al seleccionar los principales con los que compartir el dominio de multidifusión. Para obtener más información acerca de la creación de un recurso compartido, consulte Creación de un recurso compartido con AWS RAM en la Guía del usuario de AWS RAM

Contenido

Requisitos previos para compartir un dominio de multidifusión

- Para compartir un dominio de multidifusión, debes tenerlo en tu cuenta. AWS No puede compartir un dominio de multidifusión que se haya compartido con usted.
- Para compartir un dominio de multidifusión con tu organización o unidad organizativa AWS Organizations, debes habilitar el uso compartido con. AWS Organizations Para obtener más información, consulte Habilitar el uso compartido con AWS Organizations en la Guía del usuario de AWS RAM .

Servicios relacionados

El uso compartido de dominios de multidifusión se integra con AWS Resource Access Manager ()AWS RAM. AWS RAM es un servicio que le permite compartir sus AWS recursos con cualquier AWS cuenta o a través AWS Organizations de. Con AWS RAM, puede compartir recursos de su

propiedad creando un recurso compartido. Un uso compartido de recursos especifica los recursos que se compartirán y los usuarios con quienes compartirlos. Los consumidores pueden ser AWS cuentas individuales, unidades organizativas o toda una organización AWS Organizations.

Para obtener más información al respecto AWS RAM, consulte la Guía AWS RAM del usuario.

Permisos de dominio de multidifusión compartidos

Permisos de los propietarios

Los propietarios son responsables de administrar el dominio de multidifusión y los miembros y conexiones que registran o asocian con el dominio. Los propietarios pueden cambiar o revocar el acceso compartido en cualquier momento. Pueden usar AWS Organizations para ver, modificar y eliminar los recursos que los consumidores crean en dominios de multidifusión compartidos.

Permisos de los consumidores

Los usuarios del dominio de multidifusión compartido pueden realizar las siguientes operaciones en dominios de multidifusión compartidos al igual que en los dominios de multidifusión que crearon:

- Registrar y anular el registro de miembros del grupo u orígenes de grupo en el dominio de multidifusión
- Asociar una subred con el dominio de multidifusión y desasociar subredes del dominio de multidifusión

Los consumidores son responsables de administrar los recursos que crean en el dominio de multidifusión compartido.

Los clientes no pueden ver ni modificar recursos propiedad de otros consumidores o del propietario del dominio de multidifusión y no pueden modificar los dominios de multidifusión que se comparten con ellos.

Facturación y medición

No hay cargos adicionales por compartir dominios de multidifusión tanto para el propietario como para los consumidores.

Cuotas

Un dominio de multidifusión compartido cuenta para las cuotas de dominio de multidifusión tanto del propietario como del usuario con quien se compartió el dominio.

Comparta recursos entre zonas de disponibilidad en AWS Transit Gateway

Para garantizar que los recursos se distribuyan entre las zonas de disponibilidad de una región, AWS Transit Gateway asigna de forma independiente las zonas de disponibilidad a los nombres de cada cuenta. Esto podría dar lugar a diferencias de nomenclatura de zona de disponibilidad entre cuentas. Por ejemplo, es posible que la zona `us-east-1a` de disponibilidad de su AWS cuenta no tenga la misma ubicación que la `us-east-1a` de otra AWS cuenta.

Para identificar la ubicación de su dominio de multidifusión en relación con sus cuentas, debe usar el ID de zona de disponibilidad (ID de AZ). El ID de zona de disponibilidad es un identificador único y coherente de una zona de disponibilidad en todas AWS las cuentas. Por ejemplo, `use1-az1` es un ID de zona geográfica para la `us-east-1` región y se encuentra en la misma ubicación en todas las AWS cuentas.

Para ver la zona de disponibilidad IDs de las zonas de disponibilidad de su cuenta

1. Abre la AWS RAM consola en https://console.aws.amazon.com/ram/casa.
2. Las AZ IDs de la región actual se muestran en el panel Tu ID de AZ, en la parte derecha de la pantalla.

Compartir un dominio de multidifusión en AWS Transit Gateway

Cuando un propietario le comparte un dominio de multidifusión, usted puede hacer lo siguiente:

- Registrar y anular el registro de miembros del grupo u orígenes de grupo
- Asociar y desasociar subredes

> **Note**
>
> Para compartir un dominio de multidifusión, debe agregarlo a un recurso compartido. Un recurso compartido es un AWS RAM recurso que te permite compartir tus recursos entre AWS cuentas. Un recurso compartido especifica los recursos que compartir y los consumidores con quienes se comparten. Cuando compartes un dominio de multidifusión mediante el Amazon Virtual Private Cloud Console, lo agregas a un recurso compartido existente. Para agregar el dominio de multidifusión a un nuevo recurso compartido, primero debe crear el recurso compartido mediante la consola de AWS RAM.

Si forma parte de una organización AWS Organizations y está habilitado el uso compartido dentro de su organización, los consumidores de su organización tienen acceso automático al dominio de multidifusión compartido. De lo contrario, los consumidores reciben una invitación para unirse al recurso compartido y se les concede acceso al dominio de multidifusión compartido después de aceptar la invitación.

Puede compartir un dominio de multidifusión de su propiedad mediante la Amazon Virtual Private Cloud consola, la AWS RAM consola o el. AWS CLI

Para compartir un dominio de multidifusión de su propiedad mediante la *Amazon Virtual Private Cloud Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Multicast Domains (Dominios de multidifusión).
3. Seleccione el dominio de multidifusión y, a continuación, elijaActions (Acciones), Share multicast domain (Compartir dominio de multidifusión).
4. Seleccione su recurso compartido y elija Share multicast domain (Compartir dominio de multidifusión).

Para compartir un dominio de multidifusión de su propiedad mediante la consola AWS RAM

Consulte Crear un recurso compartido en la Guía del usuario de AWS RAM .

Para compartir un dominio de multidifusión de su propiedad mediante el AWS CLI

Utilice el comando create-resource-share.

Dejar de compartir un dominio de multidifusión compartido en AWS Transit Gateway

Cuando un dominio de multidifusión compartido no se comparte, sucede lo siguiente a los recursos de dominio de multidifusión del consumidor:

- Las subredes de consumidores se desasocian del dominio de multidifusión. Las subredes permanecen en la cuenta del consumidor.
- Los orígenes del grupo del consumidor y los miembros del grupo se desasocian del dominio de multidifusión y, a continuación, se eliminan de la cuenta del consumidor.

Para dejar de compartir un dominio de multidifusión, debe quitarlo del recurso compartido. Puede hacerlo desde la AWS RAM consola o desde AWS CLI.

Para dejar de compartir un dominio de multidifusión compartido de su propiedad, debe quitarlo del recurso compartido. Puede hacerlo mediante la AWS RAM consola Amazon Virtual Private Cloud, o la AWS CLI.

Para anular el uso compartido de un dominio de multidifusión compartido de su propiedad mediante la *Amazon Virtual Private Cloud Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Multicast Domains (Dominios de multidifusión).
3. Seleccione el dominio de multidifusión y, a continuación, elija Actions (Acciones), Stop sharing (Dejar de compartir).

Para dejar de compartir un dominio de multidifusión compartido de su propiedad mediante la consola AWS RAM

Consulte Actualización de un recurso compartido en la Guía del usuario de AWS RAM .

Para dejar de compartir un dominio de multidifusión compartido de tu propiedad mediante el AWS CLI

Utilice el comando disassociate-resource-share.

Identifique un dominio de multidifusión compartido en AWS Transit Gateway

Los propietarios y los consumidores pueden identificar los dominios de multidifusión compartidos mediante y Amazon Virtual Private Cloud AWS CLI

Para identificar un dominio de multidifusión compartido mediante la *Amazon Virtual Private Cloud Console

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Multicast Domains (Dominios de multidifusión).
3. Seleccione su dominio de multidifusión.
4. En la página de detalles del dominio de multidifusión de tránsito, consulte el ID de propietario para identificar el ID de AWS cuenta del dominio de multidifusión.

Para identificar un dominio de multidifusión compartido mediante el AWS CLI

Utilice el comando describe-transit-gateway-multicast-domains. El comando devuelve los dominios de multidifusión de los que es propietario y los dominios de multidifusión que comparte con usted. `OwnerId`muestra el ID de AWS cuenta del propietario del dominio de multidifusión.

Registrar fuentes con un grupo de multidifusión en AWS Transit Gateway

> **Note**
>
> Este procedimiento solo es necesario cuando se ha establecido el atributo de Static sources support (Soporte de orígenes estáticos) en enable (habilitar).

Utilice el siguiente procedimiento para registrar orígenes con un grupo de multidifusión. El origen es la interfaz de red que envía el tráfico de multidifusión.

Necesita la siguiente información antes de añadir un origen:

- El ID del dominio de multidifusión
- La IDs de las interfaces de red de las fuentes
- La dirección IP del grupo de multidifusión

Para registrar orígenes mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Seleccione el dominio de multidifusión y, a continuación, elija Actions (Acciones), Add group sources (Agregar orígenes de grupo).
4. Para la dirección IP del grupo, introduzca el bloque IPv4 CIDR o el bloque IPv6 CIDR para asignarlo al dominio de multidifusión.
5. En Choose network interfaces (Seleccionar interfaces de red), seleccione las interfaces de red de los remitentes de la multidifusión.
6. Seleccione Add sources (Agregar orígenes).

Para registrar las fuentes mediante el AWS CLI

Utilice el comando register-transit-gateway-multicast-group-sources.

Registrar miembros con un grupo de multidifusión en AWS Transit Gateway

Utilice el siguiente procedimiento para registrar miembros de grupos con un grupo de multidifusión.

Necesita la siguiente información antes de añadir miembros:

- El ID del dominio de multidifusión
- Las interfaces IDs de red de los miembros del grupo
- La dirección IP del grupo de multidifusión

Para registrar miembros mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Seleccione el dominio de multidifusión y, a continuación, elija Actions (Acciones), Add group members (Agregar miembros de grupo).
4. Para la dirección IP del grupo, introduzca el bloque IPv4 CIDR o el bloque IPv6 CIDR para asignarlo al dominio de multidifusión.
5. En Choose network interfaces (Seleccionar interfaces de red), seleccione las interfaces de red de los receptores de la multidifusión.
6. Seleccione Add members (Agregar miembros).

Para registrar miembros mediante el AWS CLI

Utilice el comando register-transit-gateway-multicast-group-members.

Anulación del registro de orígenes del grupo de multidifusión de AWS Transit Gateway

No es necesario seguir este procedimiento a menos que haya agregado manualmente un origen al grupo de multidifusión.

Para eliminar un origen mediante la consola

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

2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de gateway de tránsito).
3. Seleccione el dominio de multidifusión.
4. Seleccione la pestaña Groups (Grupos).
5. Seleccione los orígenes y, a continuación, elija Remove source (Eliminar origen).

Para eliminar un origen mediante la AWS CLI

Utilice el comando deregister-transit-gateway-multicast-group-sources.

Anular el registro de miembros de un grupo de multidifusión en Transit Gateway AWS

No es necesario seguir este procedimiento a menos que haya agregado manualmente un miembro al grupo de multidifusión.

Para anular el registro de los miembros mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Seleccione el dominio de multidifusión.
4. Seleccione la pestaña Groups (Grupos).
5. Seleccione los miembros y, a continuación, elija Remove member (Eliminar miembro).

Para anular el registro de miembros mediante el AWS CLI

Utilice el comando deregister-transit-gateway-multicast-group-members.

Ver grupos de multidifusión en AWS Transit Gateway

Puede ver información sobre sus grupos de multidifusión para comprobar que los miembros fueron detectados mediante el IGMPv2 protocolo. El tipo de miembro (en la consola) o `MemberType` (en la AWS CLI) muestra IGMP cuando AWS descubre miembros con el protocolo.

Para visualizar los grupos de multidifusión mediante la consola

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

2. En el panel de navegación, seleccione Transit Gateway Multicast (Multidifusión de puerta de enlace de tránsito).
3. Seleccione el dominio de multidifusión.
4. Seleccione la pestaña Groups (Grupos).

Para ver los grupos de multidifusión mediante el AWS CLI

Utilice el comando search-transit-gateway-multicast-groups.

En el ejemplo siguiente se muestra que el protocolo IGMP detectó miembros del grupo de multidifusión.

```
aws ec2 search-transit-gateway-multicast-groups --transit-gateway-multicast-domain tgw-mcast-domain-000fb24d04EXAMPLE
{
    "MulticastGroups": [
        {
            "GroupIpAddress": "224.0.1.0",
            "TransitGatewayAttachmentId": "tgw-attach-0372e72386EXAMPLE",
            "SubnetId": "subnet-0187aff814EXAMPLE",
            "ResourceId": "vpc-0065acced4EXAMPLE",
            "ResourceType": "vpc",
            "NetworkInterfaceId": "eni-03847706f6EXAMPLE",
            "MemberType": "igmp"
        }
    ]
}
```

Configuración de la multidifusión para Windows Server en AWS Transit Gateway

Deberá realizar pasos adicionales al configurar la multidifusión para que funcione con las puertas de enlace de tránsito en Windows Server 2019 o 2022. Para la configuración, necesitará usar PowerShell y ejecutar los siguientes comandos:

Para configurar la multidifusión para Windows Server con PowerShell

1. Cambie Windows Server para usar IGMPv2 en lugar de IGMPv3 para la pila de TCP/IP:

```
PS C:\> New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services
\Tcpip\Parameters -Name IGMPVersion -PropertyType DWord -Value 3
```

> **Note**
>
> `New-ItemProperty` es un índice de propiedad que especifica la versión de IGMP. Como IGMP v2 es la versión compatible con la multidifusión, la propiedad `Value` debe ser `3`. En lugar de editar el registro de Windows, puede ejecutar el siguiente comando para establecer la versión de IGMP en 2:
> `Set-NetIPv4Protocol -IGMPVersion Version2`

2. El firewall de Windows elimina la mayor parte del tráfico UDP de forma predeterminada. Primero tendrá que comprobar qué perfil de conexión se utiliza para la multidifusión:

```
PS C:\> Get-NetConnectionProfile | Select-Object NetworkCategory

NetworkCategory
---------------
         Public
```

3. Actualice el perfil de conexión del paso anterior para permitir el acceso a los puertos UDP necesarios:

```
PS C:\> Set-NetFirewallProfile -Profile Public -Enabled False
```

4. Reinicie la instancia EC2.
5. Pruebe su aplicación de multidifusión para asegurarse de que el tráfico fluya según lo esperado.

Ejemplo: administrar las configuraciones IGMP mediante AWS Transit Gateway

En este ejemplo, se muestra que al menos un host utiliza el protocolo IGMP para el tráfico de multidifusión. AWS crea automáticamente el grupo de multidifusión cuando recibe un mensaje `JOIN` de IGMP desde una instancia y, a continuación, agrega la instancia como miembro de este grupo. También puede añadir de forma estática hosts que no sean IGMP como miembros de un grupo mediante el. AWS CLI Cualquier instancia que se encuentre en subredes asociadas con el dominio de multidifusión puede enviar tráfico y los miembros del grupo reciben el tráfico de multidifusión.

Siga los pasos siguientes para completar la configuración:

1. Cree una VPC. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
2. Cree una subred en la VPC. Para obtener más información, consulte Crear una subred en la Guía del usuario de Amazon VPC.
3. Cree una puerta de enlace de tránsito configurada para el tráfico de multidifusión. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
4. Cree una conexión de VPC. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
5. Cree un dominio de multidifusión configurado con compatibilidad con IGMP. Para obtener más información, consulte the section called “Crear un dominio de multidifusión de IGMP”.

   Utilice los siguientes valores:

   - Habilite el soporte. IGMPv2
   - Desactive Static sources support (Compatibilidad con fuentes estáticas).
6. Cree una asociación entre subredes en la conexión de VPC de la puerta de enlace de tránsito y el dominio de multidifusión. Para obtener más información, consulte the section called “Asociación de conexiones y subredes de VPC con un dominio de multidifusión”.
7. La versión IGMP predeterminada para EC2 es. IGMPv3 Debe cambiar la versión para todos los miembros del grupo IGMP. Puede ejecutar el siguiente comando:

   ```
   sudo sysctl net.ipv4.conf.eth0.force_igmp_version=2
   ```
8. Agregue los miembros que no utilizan el protocolo IGMP al grupo de multidifusión. Para obtener más información, consulte the section called “Registrar miembros con un grupo de multidifusión”.

Ejemplo: administrar configuraciones de fuentes estáticas en AWS Transit Gateway

En este ejemplo, se agregan orígenes de multidifusión de manera estática a un grupo. Los alojamientos no utilizan el protocolo IGMP para unirse o dejar grupos de multidifusión. Debe agregar estáticamente los miembros del grupo que reciben el tráfico de multidifusión.

Siga los pasos siguientes para completar la configuración:

1. Cree una VPC. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
2. Cree una subred en la VPC. Para obtener más información, consulte Crear una subred en la Guía del usuario de Amazon VPC.
3. Cree una puerta de enlace de tránsito configurada para el tráfico de multidifusión. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
4. Cree una conexión de VPC. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
5. Cree un dominio de multidifusión configurado para que no admita IGMP y soporte para agregar orígenes estáticamente. Para obtener más información, consulte the section called “Creación de un dominio de multidifusión de origen estático”.

   Utilice los siguientes valores:

   - Deshabilita IGMPv2 el soporte.
   - Para agregar fuentes manualmente, habilite Static sources support (Compatibilidad con fuentes estáticas).

     Las fuentes son los únicos recursos que pueden enviar tráfico de multidifusión cuando el atributo está habilitado. De lo contrario, cualquier instancia que esté en subredes asociadas con el dominio de multidifusión puede enviar tráfico de multidifusión y los miembros del grupo recibirán el tráfico de multidifusión.
6. Cree una asociación entre subredes en la conexión de VPC de la gateway de tránsito y el dominio de multidifusión. Para obtener más información, consulte the section called “Asociación de conexiones y subredes de VPC con un dominio de multidifusión”.
7. Si habilita Static sources support (Compatibilidad con fuentes estáticas), agregue la fuente al grupo de multidifusión. Para obtener más información, consulte the section called “Registrar orígenes con un grupo de multidifusión”.
8. Agregue los miembros al grupo de multidifusión. Para obtener más información, consulte the section called “Registrar miembros con un grupo de multidifusión”.

Ejemplo: administrar las configuraciones estáticas de los miembros de un grupo en AWS Transit Gateway

En este ejemplo, se muestra cómo agregar miembros de multidifusión a un grupo de manera estática. Los alojamientos no pueden utilizar el protocolo IGMP para unirse o dejar grupos de multidifusión. Cualquier instancia que se encuentre en subredes asociadas al dominio de multidifusión puede enviar tráfico de multidifusión y los miembros del grupo reciben el tráfico de multidifusión.

Siga los pasos siguientes para completar la configuración:

1. Cree una VPC. Para obtener más información, consulte Crear una VPC en la Guía del usuario de Amazon VPC.
2. Cree una subred en la VPC. Para obtener más información, consulte Crear una subred en la Guía del usuario de Amazon VPC.
3. Cree una puerta de enlace de tránsito configurada para el tráfico de multidifusión. Para obtener más información, consulte the section called “Crear una puerta de enlace de tránsito”.
4. Cree una conexión de VPC. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
5. Cree un dominio de multidifusión configurado para que no admita IGMP y soporte para agregar orígenes estáticamente. Para obtener más información, consulte the section called “Creación de un dominio de multidifusión de origen estático”.

   Utilice los siguientes valores:

   - Desactivar IGMPv2 el soporte.
   - Desactive Static sources support (Compatibilidad con fuentes estáticas).
6. Cree una asociación entre subredes en la conexión de VPC de la puerta de enlace de tránsito y el dominio de multidifusión. Para obtener más información, consulte the section called “Asociación de conexiones y subredes de VPC con un dominio de multidifusión”.
7. Agregue los miembros al grupo de multidifusión. Para obtener más información, consulte the section called “Registrar miembros con un grupo de multidifusión”.

Asignación flexible de costes

De forma predeterminada, Transit Gateway utiliza un modelo de asignación de costes basado en el remitente, en el que los gastos de procesamiento de datos se asignan a la cuenta propietaria del archivo adjunto de origen. Puede crear políticas de medición personalizadas que definan qué cuentas se deben cobrar en función de las propiedades del flujo de tráfico, como los tipos de archivos adjuntos, los ID de archivos adjuntos específicos o las direcciones de red.

Las políticas de medición consisten en reglas ordenadas que se evalúan de menor a mayor número de reglas. Cuando el tráfico coincide con una regla, se cobra a la cuenta especificada de acuerdo con la configuración de la regla. Puede especificar el propietario de la cuenta para asignar los costes entre las siguientes opciones:

- Propietario del archivo adjunto de origen: los cargos se asignan a la cuenta propietaria del archivo adjunto de origen (comportamiento predeterminado)
- Propietario del archivo adjunto de destino: los cargos se asignan a la cuenta propietaria del archivo adjunto de destino
- Propietario de Transit Gateway: los cargos se asignan a la cuenta propietaria de la pasarela de tránsito

La asignación flexible de costos permite una mejor administración de costos para las organizaciones que utilizan arquitecturas de red centralizadas, lo que permite asignar los costos a las unidades de negocio o propietarios de aplicaciones apropiados, independientemente de la topología de la red.

> **Note**
>
> La asignación flexible de costos permite asignar de manera flexible el uso de los contadores y, a su vez, los costos a los titulares de cuentas que usted elija. Sin embargo, las implicaciones fiscales para AWS las cuentas pueden variar considerablemente en función de la ubicación geográfica, los patrones de uso y otros factores. Revise las implicaciones de facturación, impuestos y administración de costos para las cuentas de su AWS organización antes de habilitar esta función. Referencia: ¿Qué es AWS Billing and Cost Management?

Políticas de medición

Las políticas de medición te permiten configurar las reglas de asignación de costes para tu pasarela de tránsito a fin de controlar a qué cuentas se les cobran los costes de procesamiento y transferencia de datos en función de las propiedades del flujo de tráfico. Esta función permite mejorar las capacidades de gestión de costes y devolución de cargos para las organizaciones que utilizan arquitecturas de red centralizadas.

Una política de medición se compone de lo siguiente:

- Política de medición: el contenedor de configuración general que contiene las reglas de la política de medición. Cuando se crea, contiene una única entrada de política de medición predeterminada que está configurada para cobrar todo el tráfico al propietario del archivo adjunto de origen. Cada pasarela de tránsito solo puede tener una política de medición.
- Introducción a la política de medición: reglas individuales dentro de una política de medición que definen los criterios de coincidencia específicos y el uso de la cuenta al contador. Cada entrada incluye un número de regla para el orden de evaluación, las condiciones de coincidencia del tráfico (como los tipos de adjuntos de origen y destino, los identificadores de los adjuntos, los bloques de CIDR, los puertos y los protocolos) y a qué propietario de la cuenta se debe cobrar por el tráfico coincidente. Una política puede contener hasta 50 entradas, evaluadas en orden del número de regla más bajo al más alto.

  Puede asignar el uso de los contadores a cualquiera de las siguientes opciones:

  - Propietario del archivo adjunto de origen: asigna el uso de la medición a la cuenta propietaria del archivo adjunto donde se origina el tráfico (comportamiento predeterminado)
  - Propietario del archivo adjunto de destino: asigna el uso de la medición a la cuenta propietaria del archivo adjunto donde termina el tráfico, y
  - propietario de la pasarela de tránsito: asigna el uso de la medición a la cuenta propietaria de la pasarela de tránsito.
- Archivos adjuntos Middlebox: accesorios de pasarela de tránsito designados (opcionales) que enrutan el tráfico a través de los dispositivos de red para la inspección de seguridad, el equilibrio de carga u otras funciones de la red. El uso de datos del tráfico que pasa por los archivos adjuntos de middlebox se mide en función del propietario de la cuenta especificado en la política de medición. Puede especificar un máximo de 10 archivos adjuntos en el cuadro intermedio. Los tipos de adjuntos de middlebox admitidos son los adjuntos de función de AWS red (Network Firewall), VPC y VPN.

Cómo funcionan las políticas de medición

De forma predeterminada, Transit Gateway utiliza un modelo de asignación de costes basado en el remitente, en el que los gastos de procesamiento de datos se repercuten en la cuenta propietaria del archivo adjunto de origen. Con las políticas de medición, puedes crear reglas personalizadas para medir el uso de manera flexible en función de las siguientes propiedades del flujo de tráfico:

- Tipos de adjuntos de origen y destino (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function y VPN Concentrator)
- ID de los adjuntos de origen y destino
- Direcciones IP de origen y destino, intervalos de puertos y protocolos

Las políticas de medición consisten en reglas ordenadas que se evalúan del número de regla más bajo al más alto. Cuando el tráfico coincide con una regla, se cobra a la cuenta especificada de acuerdo con la configuración de la cuenta medida de la regla. Las políticas de medición abordan varios escenarios organizativos comunes:

- Asignación de costos en entornos híbridos: asigne los costos AWS de ingreso de datos desde las instalaciones a través de Direct Connect Gateway al propietario de la cuenta de VPC de destino, en lugar de al propietario de la cuenta del administrador de TI central.
- Arquitectura de inspección centralizada: asigne los costos a los propietarios de aplicaciones individuales o cuentas de VPC en lugar de al equipo de seguridad central para el tráfico que atraviesa las VPC de inspección.
- Application-based contracargo: asigne todos los costos de uso de datos de una carga de trabajo al propietario de la VPC, independientemente de la dirección del tráfico.
- Asignación de costes por cliente: asigne los costes de datos a las cuentas de los clientes cuando creen archivos adjuntos a su pasarela de transporte.

Adjuntos de Middlebox

Las políticas de medición de Transit Gateway admiten los archivos adjuntos de Middlebox, lo que le permite asignar de manera flexible los cargos de procesamiento de datos al tráfico de red enrutado a través de dispositivos Middlebox, como firewalls de red y balanceadores de carga. Algunos ejemplos de adjuntos middlebox son los adjuntos de función de red a AWS Network Firewall o los adjuntos de VPC que redirigen el tráfico a dispositivos de seguridad de terceros en una VPC. El tráfico entre los adjuntos de las pasarelas de tránsito de origen y destino pasa por estos adjuntos intermedios para

los casos de uso típicos de las inspecciones de seguridad. Puede definir políticas de medición para asignar de manera flexible el uso del procesamiento de datos en los archivos adjuntos intermedios al archivo adjunto de origen, al archivo adjunto de destino final o al propietario de la cuenta de Transit Gateway. En el caso de los archivos adjuntos de AWS Network Function, los gastos de procesamiento de datos del Network Firewall también se asignan a la cuenta de pago.

Asignación flexible de costos: medición de los tipos de uso

La asignación flexible de costos mediante políticas de medición se aplica a los siguientes tipos de uso de datos:

- Uso del procesamiento de datos de Transit Gateway en archivos adjuntos de VPC, VPN, Client VPN, VPN Concentrator y Direct Connect
- Uso de Client VPN Data Transfer Out en los archivos adjuntos de Client VPN
- Site-to-site Uso de transferencia de datos de VPN en archivos adjuntos de VPN
- Uso de transferencia de datos de Direct Connect en los archivos adjuntos de Direct Connect.
- Uso de la transferencia de datos en los archivos adjuntos de emparejamiento de TGW
- Transit Gateway: uso del procesamiento de datos en los archivos adjuntos con funciones de red
- AWS Uso del procesamiento de datos del firewall de red (NFW) en los archivos adjuntos de la función de red.

La asignación flexible de costos no se aplica al uso por hora de los archivos adjuntos ni al uso del procesamiento de datos de multidifusión. En el caso de los adjuntos de Transit Gateway Connect, se puede definir una política de medición para la VPC de transporte subyacente o el adjunto de Direct Connect. En el caso de los adjuntos de VPN con IP privada, se puede definir una política de medición para el adjunto Direct Connect de transporte subyacente.

Consideraciones y limitaciones

Tenga en cuenta lo siguiente al implementar políticas de medición para su pasarela de tránsito.

Permisos

- Solo el propietario de la pasarela de transporte público puede crear, modificar o eliminar las políticas de medición.
- La configuración de asignación de costos se aplica a nivel de pasarela de tránsito.

- Los propietarios de los archivos adjuntos no pueden anular los ajustes de asignación de costes configurados por el propietario de la pasarela de transporte.

Interconexión Transit Gateway

Cuando el tráfico atraviesa las conexiones de interconexión de Transit Gateway:

- Cada pasarela de tránsito aplica su propia política de medición de forma independiente.
- Cada pasarela de tránsito asigna los cargos por datos por separado en función de su política local.
- El tráfico se puede considerar como dos flujos separados: el enlace de origen al enlace de interconexión y el enlace de interconexión al destino.

Integración de WAN en la nube

Cuando una puerta de enlace de tránsito está conectada a una red principal de Cloud WAN:

- Los cargos de transferencia de datos de las pasarelas de tránsito en las conexiones entre pares se asignan de acuerdo con la política de medición de las pasarelas de tránsito.
- Las políticas de medición no son compatibles con las redes principales de Cloud WAN.

Impacto en el rendimiento

- Las políticas de medición no introducen ninguna latencia adicional en las rutas de datos.
- Las políticas de medición no afectan al ancho de banda máximo por archivo adjunto.
- No hay cambios en las capacidades de intercambio de recursos de Transit Gateway.

Integración de facturación

- Las etiquetas de asignación de costos siguen funcionando con las políticas de medición para organizar los costos por unidad de negocio.
- Las políticas de medición definen qué cuentas incurren en costos, mientras que las etiquetas de asignación de costos ayudan a categorizar esos costos.
- Los cambios en las políticas de medición entran en vigor al final de la siguiente hora de facturación.

Compatibilidad con IPv6

Las políticas de medición se admiten tanto para el tráfico IPv4 como para el IPv6. La coincidencia de bloques CIDR en las entradas de políticas funciona con ambas familias de direcciones.

Soporte para archivos adjuntos de Middlebox

- La política de medición de Middlebox asume que el tráfico entre el archivo adjunto de origen y el de destino se controla mediante el archivo adjunto especificado en el medio (por ejemplo, una inspección de tráfico de este a oeste). VPC-to-VPC Por lo tanto, las cinco tuplas de la red (source/destination IP, source/destination puertos y protocolo) para los flujos que entran y salen de los archivos adjuntos del cuadro central deben coincidir. Los flujos con 5 tuplas que no coinciden en los archivos adjuntos del cuadro central (por ejemplo, la transformación de NAT en la VPC de inspección) se tratan como flujos de archivos adjuntos de origen y destino normales (a diferencia de los flujos de archivos adjuntos del cuadro central).
- Todos los flujos de solo salida del adjunto de la caja intermedia (por ejemplo, el tráfico norte-sur a Internet a través de una IGW en una VPC de inspección) se tratan como flujos de origen y destino normales (a diferencia de los flujos de adjuntos de la caja intermedia).
- En el caso de los archivos adjuntos a las funciones de red, cuando el firewall AWS de red descarta paquetes, todo el uso de procesamiento de datos se carga a la cuenta del remitente, independientemente de la configuración de la política de medición.

Cree una política de medición de AWS Transit Gateway

Para habilitar las políticas de medición, debe crear una política de medición para su pasarela de transporte y configurar las entradas de política que definan cómo se asigna el uso de los contadores. La política de medición establece el marco y la configuración predeterminada, mientras que las entradas de la política contienen las reglas específicas que determinan qué cuentas se miden en función de las características del tráfico.

Las entradas de la política de contadores funcionan como reglas ordenadas que se aplican secuencialmente desde el número de reglas más bajo al más alto para el tráfico que circula por su pasarela de transporte. Cada entrada define los criterios de coincidencia, como los tipos de adjuntos de origen y destino, los bloques de CIDR, los protocolos y los rangos de puertos, además de la cuenta que debe medirse para determinar el tráfico coincidente. Cuando un flujo de tráfico coincide con varias entradas, prevalece la entrada con el número de regla más bajo. Si ninguna entrada coincide con un flujo concreto, se cobrará a la cuenta contabilizada predeterminada especificada en la política.

Tras crear una política, tendrá que añadir entradas de política para implementar la lógica de asignación de costes. Para conocer los pasos para crear una entrada de política de medición, consulteCree una entrada de política de medición.

Cree una política de medición mediante la consola

Cree una política para definir reglas flexibles de asignación de costos para el uso de datos de las pasarelas de tránsito. De forma predeterminada, todos los flujos se miden en función del propietario del archivo adjunto de origen. Cree entradas para facturar flujos de red específicos a diferentes cuentas.

Para crear una política de medición

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Políticas de medición.
3. Seleccione Crear política de medición.
4. En el campo ID de la pasarela de transporte, elige la pasarela de transporte para la que quieres crear la política de medición.
5. (Opcional) Para el accesorio Middlebox IDs, elige uno o más accesorios Middlebox. De forma predeterminada, el uso de datos se mide en función del propietario del middlebox. La compatibilidad con los archivos adjuntos de Middlebox permite aplicar una política de medición al tráfico que atraviesa los archivos adjuntos de Middlebox. Se pueden añadir archivos adjuntos adicionales más adelante.
6. (Opcional) En la sección Etiquetas, añada etiquetas para ayudarle a identificar y organizar su política de medición:
   a. Elija Añadir nueva etiqueta.
   b. Introduzca una clave de etiqueta y, si lo desea, un valor de etiqueta.
   c. Seleccione Agregar nueva etiqueta para agregar etiquetas adicionales o avance al siguiente paso. Puede añadir hasta 50 etiquetas.
7. Selecciona Crear una política de medición de Transit Gateway.

> **Note**
>
> La cuenta de medición predeterminada es la propietaria del archivo adjunto de origen y, tras crear una política de medición, puede añadir entradas que definan qué cuenta se cobrará en

función de las propiedades del flujo de tráfico, teniendo en cuenta que la entrada de política predeterminada (que es la última entrada) no se puede modificar ni eliminar como otras entradas de política.

Cree una política de medición mediante el AWS CLI

Una política de medición define el comportamiento de asignación de costes y la configuración global predeterminados de tu pasarela de transporte público. Usa la políticacreate-transit-gateway-metering.

Parámetros requeridos:

- `--transit-gateway-id`- El ID de la pasarela de tránsito para la que se va a crear la política

Parámetros opcionales:

- `--middle-box-attachment-ids`- Se admiten los identificadores adjuntos de la pasarela de tránsito para añadirlos a la política como servidor intermedio
- `--tag-specifications`- etiquetas para la política de medición

Para crear una política de medición utilizando el AWS CLI

1. Ejecute el create-transit-gateway-metering-policy comando para crear una nueva política de medición con adjuntos opcionales en el cuadro intermedio.

```
aws ec2 create-transit-gateway-metering-policy \
    --transit-gateway-id tgw-07a5946195a67dc47 \
    --middle-box-attachment-ids \
    tgw-attach-0123456789abcdef0 \
    tgw-attach-0abc123def456789a \
    --tag-specifications \
    '[{ "ResourceType": "transit-gateway-metering-policy", \
    "Tags": [ { "Key": "Env", "Value": "Prod" } ] }]'
```

   Este comando crea una política de medición para la pasarela de tránsito especificada con las etiquetas y los archivos adjuntos incluidos en el cuadro intermedio.
2. El comando devuelve el siguiente resultado cuando la política se ha creado correctamente:

```
{
```

```
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0abc123def456789a"],
        "State": "pending",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z",
        "Tags": [{"Key": "Env","Value": "Prod"}]
    }
}
```

Anote el ID de la política de medición devuelto en la respuesta para usarlo en comandos posteriores. describe-transit-gateway-metering-policiesEl comando se puede utilizar para obtener la política de medición asociada a la pasarela de tránsito.

Gestione las AWS políticas de medición de Transit Gateway

Después de crear una política de medición, puede administrarla consultando la configuración actual, modificando las opciones de configuración o eliminando la política cuando ya no sea necesaria. Las operaciones de administración le permiten añadir o eliminar adjuntos intermedios a medida que cambien los requisitos de la red. Solo puede crear o eliminar una entrada de política. Si necesita modificar una regla existente, puede eliminar la entrada y crear una nueva con la configuración modificada. Todas las operaciones de administración requieren los permisos del propietario de la pasarela de tránsito y entran en vigor después de dos horas de facturación.

La administración eficaz de las políticas de medición es crucial para mantener una asignación de costos precisa a medida que la arquitectura de la red evoluciona. A menudo, las organizaciones necesitan ajustar sus políticas cuando las unidades de negocio cambian, se implementan nuevas aplicaciones o se modifican las topologías de red. Por ejemplo, es posible que la configuración de compatibilidad con la medición intermedia requiera actualizaciones cuando cambien las arquitecturas de seguridad de los firewalls o cuando se introduzcan nuevos servicios de inspección en la ruta de tráfico.

Las modificaciones de las políticas son compatibles con varios escenarios operativos, como los cambios estacionales en los patrones de tráfico, las actividades de fusiones y adquisiciones y las actualizaciones de los requisitos de conformidad. Al gestionar las políticas, tenga en cuenta el impacto en los acuerdos de facturación existentes y comunique los cambios a las partes interesadas afectadas antes de su implementación.

Las revisiones periódicas de las políticas ayudan a garantizar que la asignación de costos se mantenga alineada con los objetivos empresariales y las estructuras organizativas. Las mejores prácticas incluyen documentar los cambios en las políticas, probar las modificaciones en entornos no productivos siempre que sea posible y coordinarse con los equipos financieros para comprender las implicaciones de la facturación. Además, tenga en cuenta el calendario de los cambios en las políticas para minimizar las interrupciones en los ciclos de facturación mensuales y los procesos de presentación de informes financieros.

Temas

Editar una política de medición de AWS Transit Gateway

Edite las políticas de medición existentes para modificar las configuraciones de los accesorios de la cámara intermedia. Las modificaciones de la política entrarán en vigor a la siguiente hora de facturación y se aplicarán a todos los flujos de tráfico futuros a través de tu pasarela de transporte público.

Edita una política de medición mediante la consola

Usa la consola para modificar la configuración de la política de medición existente en tu pasarela de transporte público.

Para editar una política de medición existente mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Políticas de medición.
3. Seleccione la política de medición que desee modificar eligiendo su ID de política
4. Modifique la configuración de política disponible en Acciones. La consola solo permite añadir y eliminar archivos adjuntos del cuadro central.

    - Adjuntos de tipo middlebox: añada o elimine los archivos adjuntos de Transit Gateway, que deberían considerarse cajas intermedias para la facturación especializada.

Edite una política de medición mediante el AWS CLI

Utilice el modify-transit-gateway-metering-policy comando para ver y modificar las políticas de medición.

Parámetros necesarios para modificar las operaciones:

- `--transit-gateway-metering-policy-id`- El ID de la política de medición que se va a modificar
- `--add-middle-box-attachment-ids` o `--remove-middle-box-attachment-ids` - Se admiten los identificadores adjuntos de las pasarelas de tránsito para añadirlos o eliminarlos de la política como intermediario

Para ver y editar las políticas de medición mediante la CLI AWS

1. (Opcional) Vea las políticas de medición existentes mediante el describe-transit-gateway-metering-policies comando para ver los ajustes de configuración actuales:

   ```
   aws ec2 describe-transit-gateway-metering-policies
   ```

   Este comando devuelve todas las políticas de medición de su cuenta, muestra su estado actual y los archivos adjuntos están habilitados como intermediario para cada una de las políticas de medición.
2. Modifique una política de medición mediante el modify-transit-gateway-metering-policy comando para actualizar las opciones de configuración:

   ```
   aws ec2 modify-transit-gateway-metering-policy \
       --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
       --add-middle-box-attachment-ids tgw-attach-0123456789abcdef1  \
       --remove-middle-box-attachment-ids tgw-attach-0abc123def456789a
   ```

   Este comando modifica una política de medición añadiendo y and/or eliminando los adjuntos del cuadro intermedio.
3. El comando devuelve el siguiente resultado cuando la política se modifica correctamente:

   ```
   {
       "TransitGatewayMeteringPolicy": {
           "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
   ```

```
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "modifying",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

Los cambios pueden tardar hasta dos horas de facturación en surtir efecto.

Eliminar una política de medición de AWS Transit Gateway

Elimine las políticas de medición cuando ya no sean necesarias para su estrategia de asignación de costos de Transit Gateway. Al eliminar una política, se restablece la asignación de costos al modelo predeterminado basado en el remitente, en el que los cargos por procesamiento y transferencia de datos se asignan a la cuenta propietaria del archivo adjunto de origen. También se eliminan todas las entradas de política asociadas a la política de medición eliminada.

Elimine una política de medición mediante la consola

Utilice la consola para eliminar las políticas de medición que ya no sean necesarias.

Para eliminar una política de medición mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Políticas de medición.
3. Seleccione la política que desee eliminar eligiendo su ID de política.
4. Elija Actions (Acciones) y, a continuación, elija Delete (Eliminar).
5. Confirme la eliminación escribiendo **`delete`** en el cuadro de diálogo de confirmación.
6. Elija Eliminar.

> **Important**
>
> La eliminación de una política de medición es irreversible. Todas las entradas de la política y los ajustes de configuración se eliminarán permanentemente y la asignación de costes volverá al modelo predeterminado basado en el remitente.

Elimine una política de medición mediante el AWS CLI

Utilice el delete-transit-gateway-metering-policy comando para eliminar las políticas de medición mediante programación.

Requisitos:

- Permisos de propietario de la pasarela de tránsito

Parámetros requeridos:

- `--transit-gateway-metering-policy-id`- El ID de la política de medición que se va a eliminar

Para ver y eliminar las políticas de medición mediante la CLI AWS

1. (Opcional) Vea las políticas de medición existentes mediante el describe-transit-gateway-metering-policies comando para ver los ajustes de configuración actuales:

   ```
   aws ec2 describe-transit-gateway-metering-policies
   ```

   Este comando devuelve todas las políticas de medición de su cuenta y muestra su estado y configuración actuales.
2. Elimine una política de medición mediante el delete-transit-gateway-metering-policy comando para eliminarla permanentemente:

   ```
   aws ec2 delete-transit-gateway-metering-policy \
       --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7
   ```

   Este comando elimina permanentemente la política de medición especificada y todas las entradas asociadas. La asignación de costos volverá al modelo predeterminado basado en el remitente para todos los flujos de tráfico futuros. Este cambio también tarda 2 horas en aplicarse a la facturación.
3. El comando devuelve el siguiente resultado cuando la política se elimina correctamente:

   ```
   {
       "TransitGatewayMeteringPolicy": {
           "TransitGatewayMeteringPolicyId": "tgw-mp-042d444564d4b2da7",
   ```

```
        "TransitGatewayId": "tgw-07a5946195a67dc47",
        "MiddleboxAttachmentIds":  ["tgw-attach-0123456789abcdef0",
        "tgw-attach-0123456789abcdef1"],
        "State": "deleting",
        "UpdateEffectiveAt": "2025-11-05T21:00:00.000Z"
    }
}
```

La respuesta confirma que la política se está eliminando con un `deleting` estado mientras la eliminación se procesa en la infraestructura de Transit Gateway.

Crea un AWS Entrada a la política de medición de Transit Gateway

De forma predeterminada, todos los flujos se miden en función del propietario del archivo adjunto de origen. Para medir flujos específicos a diferentes cuentas, cree entradas de política individuales que definan a qué cuenta se le cobrará en función de las propiedades del flujo de tráfico.

Las entradas de las políticas de medición funcionan como reglas condicionales que se evalúan en orden secuencial en función de sus números de regla cuando el tráfico pasa por la pasarela de transporte público. Cada entrada actúa como una afirmación «si, entonces»: si el tráfico coincide con los criterios especificados (como el tipo de archivo adjunto de origen, el bloque CIDR de destino o el protocolo), cargue el importe a la cuenta designada. El sistema evalúa las entradas desde el número de regla más bajo hasta el más alto, y la primera entrada coincidente determina la cuenta de facturación de ese flujo de tráfico.

Las entradas admiten una amplia gama de criterios de coincidencia, incluidos los tipos de adjuntos (VPC, VPN, Client VPN, Direct Connect Gateway, Peering, Network Function y VPN Concentrator), ID de adjuntos específicos, bloques CIDR de origen y destino, tipos de protocolos e intervalos de puertos. Puede combinar varios criterios en una sola entrada para crear reglas de segmentación precisas. Por ejemplo, puedes crear una entrada que coincida con todo el tráfico HTTPS (puerto 443) de los archivos adjuntos de la VPC a un rango de CIDR de destino específico y que cargue esos flujos a la cuenta de un equipo de seguridad. Si ninguna entrada coincide con un flujo de tráfico concreto, se cobrará a la cuenta de contador predeterminada especificada en la política de medición principal, para garantizar que todo el tráfico se facture correctamente. La creación de una entrada tarda 2 horas en surtir efecto.

> **Important**
>
> - Planifique los números de las reglas con cuidado: deje espacios vacíos (por ejemplo, 10, 20, 30) para permitir inserciones futuras
> - Pruebe primero las entradas con condiciones menos específicas antes de añadir reglas más restrictivas
> - Utilice condiciones de coincidencia específicas para evitar la facturación no intencionada

Cree una entrada de política de medición mediante la consola

Una política de medición define el comportamiento de asignación de costes y la configuración global predeterminados de tu pasarela de transporte público.

Para crear una entrada de política de medición mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Políticas de medición.
3. Seleccione el enlace del identificador de la política de medición para ver sus detalles.
4. Seleccione la pestaña de entradas de la política de medición.
5. Seleccione Crear entrada de política de medición.
6. Número de regla de política: debe ser un número único (1- 32.766) que determine el orden de evaluación. Los números más bajos tienen mayor prioridad.
7. Cuenta con taxímetro: elige uno de los siguientes tipos de cuentas para que se te cobre por los flujos de tráfico coincidentes:
   a. Fuente: propietario del archivo adjunto
   b. Propietario del archivo adjunto de destino
   c. Propietario del archivo adjunto de Transit Gateway
8. (Opcional) Elija las condiciones de la regla: estas condiciones opcionales definen los criterios que se ajustan al tráfico específico:
   - ID o tipo de archivo adjunto de origen: filtre por tipo de archivo adjunto (VPC, VPN, Client VPN, Direct Connect Gateway, peering, función de red y concentrador de VPN) o ID.
   - Tipo o ID de archivo adjunto de destino: filtre por tipo o ID de archivo adjunto de destino

- Bloqueo CIDR de origen: haga coincidir el tráfico de rangos de IP específicos
- Bloque CIDR de destino: relaciona el tráfico con rangos de IP específicos
- Rango de puertos de origen: coincide con puertos de origen específicos
- Rango de puertos de destino: coincide con puertos de destino específicos
- Protocolo: filtra por protocolo para la regla (1, 6, 17, etc.)

9. Seleccione Crear entrada de política de medición para guardar la configuración.

Cree una entrada de política de medición mediante el AWS CLI

Las entradas de políticas definen reglas específicas para la asignación de costos en función de las características del tráfico. Las reglas se evalúan en orden del número de regla más bajo al más alto.

Parámetros requeridos:

- `--transit-gateway-metering-policy-id`- El ID de la política de medición a la que se va a añadir la entrada
- `--policy-rule-number`- Un número único (del 1 al 32 766) que determina el orden de evaluación
- `--metered-account`- tipo de pagador (propietario del archivo adjunto de origen, propietario del archivo adjunto de destino, propietario de la puerta de enlace de tránsito)

Parámetros opcionales:

Estos parámetros opcionales que definen los criterios para que coincidan con un tráfico específico:

- `--source-transit-gateway-attachment-id`- El ID del adjunto de la pasarela de tránsito de origen.
- `--source-transit-gateway-attachment-type`- El tipo de adjunto a la pasarela de tránsito de origen.
- `--source-cidr-block`- El bloque CIDR de origen de la regla.
- `--source-port-range`- El rango de puertos de origen de la regla.
- `--destination-transit-gateway-attachment-id`- El ID del adjunto a la pasarela de tránsito de destino.
- `--destination-transit-gateway-attachment-type`- El tipo de adjunto a la pasarela de tránsito de destino.

- `--destination-cidr-block`- El bloque CIDR de destino de la regla.
- `--destination-port-range`- El rango de puertos de destino de la regla.
- `--protocol`- El número de protocolo de la regla

Para crear una entrada de política de medición mediante el AWS CLI

1. Usa el create-transit-gateway-metering-policy-entry comando para crear una nueva entrada de política que enrute el tráfico de VPC a una cuenta medida específica:

   ```
   aws ec2 create-transit-gateway-metering-policy-entry \
       --transit-gateway-metering-policy-id tgw-mp-042d444564d4b2da7 \
       --policy-rule-number 100 \
       --destination-transit-gateway-attachment-type vpc \
       --metered-account destination-attachment-owner
   ```

   Este comando crea una entrada de política con la regla número 100 que coincide con el tráfico destinado a los adjuntos de VPC y cobra al propietario del adjunto de destino por esos flujos.
2. El comando devuelve el siguiente resultado cuando la entrada se crea correctamente:

   ```
   {
       "TransitGatewayMeteringPolicyEntry": {
           "MeteredAccount": "destination-attachment-owner",
           "MeteringPolicyRule": {
               "DestinationTransitGatewayAttachmentType": "vpc"
           },
           "PolicyRuleNumber": 100,
           "State": "available",
           "UpdateEffectiveAt": "2025-11-06T02:00:00.000Z"
       }
   }
   ```

   La respuesta confirma que la entrada se creó con un estado «disponible» mientras se activaba en la infraestructura de Transit Gateway.

Eliminar una entrada de la política de medición de AWS Transit Gateway

Elimine las entradas de la política de medición cuando ya no se requieran reglas específicas de asignación de costos para los flujos de tráfico de su red. La eliminación de entradas ayuda a

simplificar la administración de políticas al eliminar las reglas obsoletas o innecesarias y, al mismo tiempo, mantener la estructura general de las políticas. Al eliminar una entrada, el tráfico que anteriormente coincidía con la regla eliminada se evaluará comparándolo con las entradas restantes en orden numérico de regla, o volverá al comportamiento predeterminado de la política si ninguna otra entrada coincide.

Antes de eliminar las entradas, tenga en cuenta el impacto en los acuerdos de facturación y los flujos de tráfico actuales. Una vez eliminado, el cambio tarda hasta 2 horas en hacerse efectivo y no se puede deshacer, así que coordine los cambios con los propietarios de las cuentas y los equipos financieros afectados. Revisa las entradas restantes para asegurarte de que la cobertura del tráfico y la asignación de la facturación sean adecuadas tras la eliminación. El orden de evaluación de las reglas para las entradas restantes permanece sin cambios, lo que permite mantener un comportamiento predecible de asignación de costos para los flujos de tráfico continuos.

⚠ Important

- La eliminación es irreversible
- El tráfico que anteriormente coincidiera con esta entrada se volverá a evaluar comparándolo con las entradas restantes
- Revise las entradas restantes para garantizar una cobertura de tráfico adecuada

Elimine una entrada de la política de medición mediante la consola

Utilice la consola para eliminar entradas de políticas a través de una interfaz intuitiva que proporciona cuadros de diálogo de confirmación para evitar eliminaciones accidentales.

Para eliminar una entrada de política mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Políticas de medición.
3. Seleccione la política de medición que contiene la entrada que desea eliminar.
4. Seleccione la entrada que desee eliminar y elija Eliminar.
5. En el cuadro de diálogo de confirmación, revise los detalles de la entrada y escriba **`delete`** para confirmar la eliminación.
6. Seleccione Eliminar para eliminar permanentemente la entrada.

Elimine una entrada de política de medición mediante el AWS CLI

Utilice el delete-transit-gateway-metering-policy-entry comando para eliminar las entradas de la política mediante programación.

Requisitos:

- Permisos de propietario de Transit Gateway
- ID de política de medición válido y número de regla de entrada

Parámetros requeridos:

- `--transit-gateway-metering-policy-id`- El ID de la política de medición
- `--policy-rule-number`- El número de regla de la entrada que se va a eliminar

Para ver y eliminar entradas de políticas mediante la AWS CLI

1. (Opcional) Vea las entradas de políticas existentes mediante el get-transit-gateway-metering-policy-entries comando para ver los ajustes de configuración actuales:

   ```
   aws ec2 get-transit-gateway-metering-policy-entries \
       --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg
   ```

   Este comando devuelve todas las entradas de la política especificada y muestra los números de regla, los criterios coincidentes y las cuentas contabilizadas.
2. Elimine una entrada de política mediante el delete-transit-gateway-metering-policy-entry comando para eliminarla permanentemente:

   ```
   aws ec2 delete-transit-gateway-metering-policy-entry \
       --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
       --policy-rule-number 100
   ```

   Este comando elimina permanentemente la entrada especificada de la política. El tráfico que anteriormente coincidía con esta entrada se reevaluará inmediatamente comparándolo con las entradas restantes o volverá al comportamiento predeterminado de la política.
3. El comando devuelve el siguiente resultado cuando la entrada se elimina correctamente:

```
{
    "TransitGatewayMeteringPolicyEntry": [
        {
            "PolicyRuleNumber": 100,
            "MeteredAccount": "destination-attachment-owner",
            "UpdateEffectiveAt": "2024-01-01T01:00:00+00:00",
            "state": "deleted",
            "MeteringPolicyRule": {
                "DestinationTransitGatewayAttachmentType": "vpc"
            }
        }
}
```

La respuesta confirma que la entrada se está eliminando con el estado «eliminada» mientras la eliminación se procesa en la infraestructura de Transit Gateway.

Administre los AWS archivos adjuntos de middlebox de la política de medición de Transit Gateway

Las políticas de medición de Transit Gateway son compatibles con los archivos adjuntos de Middlebox, lo que le permite asignar de manera flexible los cargos de procesamiento de datos al tráfico de red enrutado a través de dispositivos Middlebox, como firewalls de red y balanceadores de carga. Algunos ejemplos de adjuntos de middlebox son los adjuntos de función de red a AWS Network Firewall o los adjuntos de VPC que redirigen el tráfico a dispositivos de seguridad de terceros en una VPC. El tráfico entre los adjuntos de las pasarelas de tránsito de origen y destino pasa por estos adjuntos intermedios para los casos de uso típicos de las inspecciones de seguridad. Puede definir políticas de medición para asignar de manera flexible el uso del procesamiento de datos en los archivos adjuntos intermedios al archivo adjunto de origen, al archivo adjunto de destino final o al propietario de la cuenta de Transit Gateway. En el caso de los archivos adjuntos de AWS Network Function, los gastos de procesamiento de datos del Network Firewall también se asignan a la cuenta de pago.

Adjuntos de pasarela de tránsito designados que enrutan el tráfico a través de los dispositivos de red para la inspección de seguridad, el equilibrio de carga u otras funciones de la red. El uso de datos del tráfico que atraviesa los archivos adjuntos de la cámara intermedia se mide en función del propietario de la cuenta especificado en la política de medición. Puede especificar un máximo de 10 archivos

adjuntos en el cuadro intermedio. Los tipos de adjuntos de middlebox admitidos son los adjuntos de función de AWS red (Network Firewall), VPC y VPN.

Temas

Agregue archivos adjuntos en el cuadro intermedio de la política de medición de AWS Transit Gateway

Puede añadir accesorios middlebox para integrar los dispositivos de red en su política de medición de Transit Gateway. Esto te permite enrutar tráfico específico a través de dispositivos de seguridad, balanceadores de carga u otras funciones de la red y, al mismo tiempo, mantener un control detallado de la asignación de costos.

> **Important**
>
> - Asegúrese de que los dispositivos middlebox estén correctamente configurados y sean accesibles
> - Pruebe el enrutamiento del tráfico antes de aplicarlo a las cargas de trabajo de producción
> - Supervise el rendimiento de la cámara intermedia para evitar introducir latencia
> - Configure el comportamiento de conmutación por error adecuado para una alta disponibilidad

Añada los accesorios de middlebox mediante la consola

Para añadir una entrada de archivos adjuntos de middlebox

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Políticas de medición.
3. Seleccione el enlace del identificador de la política de medición para ver sus detalles.
4. Seleccione la pestaña de adjuntos de Middlebox.
5. Elija Agregar.

6. Cuando se le solicite, seleccione el adjunto de la caja intermedia IDs que debe tratarse como una caja intermedia para la facturación especializada. Puede seleccionar hasta 10 archivos adjuntos de tipo middlebox.
7. Seleccione Añadir archivos adjuntos en el cuadro intermedio para guardar la configuración.

Añada los adjuntos de middlebox mediante el AWS CLI

Utilice el modify-transit-gateway-metering-policy comando para añadir archivos adjuntos.

Antes de empezar, asegúrese de tener los siguientes parámetros obligatorios:

- `--transit-gateway-metering-policy-id`- El identificador de la política de medición existente
- `--add-middle-box-attachment-ids`- Uno o más archivos adjuntos IDs para añadir a la política (para añadir archivos adjuntos)

Para agregar adjuntos de middlebox a una política existente mediante la CLI AWS

1. En el siguiente ejemplo, modify-transit-gateway-metering-policy se usa para agregar cuatro adjuntos intermedios a una política de medición existente. El comando añade el adjunto especificado IDs a la lista existente sin eliminar los adjuntos actuales:

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --add-middle-box-attachment-ids tgw-attach-0bdc681c211bf71f3 tgw-
attach-0987654321fedcba0 tgw-attach-0456789012345abcd tgw-attach-0fedcba0987654321
```

2. En el siguiente ejemplo de respuesta, el resultado de JSON muestra la configuración de política actualizada con los cuatro archivos adjuntos del cuadro intermedio ahora incluidos:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0",
            "tgw-attach-0456789012345abcd",
            "tgw-attach-0fedcba0987654321"
        ],
```

```
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

Elimine los AWS archivos adjuntos del cuadro intermedio de la política de medición de Transit Gateway

De forma predeterminada, los costos de medición se atribuyen al propietario del accesorio de la caja intermedia. Sin embargo, puede modificar estas asignaciones para garantizar que los costos se asignen correctamente al origen o destino real del tráfico. Puede añadir o eliminar hasta un total de 10 adjuntos intermedios para una política de medición.

Quite los accesorios de la caja intermedia con la consola

Utilice la consola de Amazon VPC para eliminar los adjuntos de middlebox de la configuración de su política de medición.

Para eliminar los archivos adjuntos de la caja intermedia

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, selecciona Transit Gateways, Metering policies.
3. Seleccione la política de medición que desee modificar.
4. Seleccione la pestaña de adjuntos de Middlebox.
5. Seleccione un máximo de 10 adjuntos de tipo middlebox para eliminarlos de la política de medición.
6. Elija Eliminar .
7. Cuando se le solicite, puede actualizar los archivos adjuntos del cuadro intermedio que haya elegido para eliminarlos. El tráfico que pase por los archivos adjuntos retirados se medirá al propietario del adjunto de la caja intermedia.
8. Selecciona Eliminar los archivos adjuntos de la caja intermedia.

Quite los accesorios de la caja intermedia utilizando el AWS CLI

Utilice el modify-transit-gateway-metering-policy comando para eliminar los archivos adjuntos.

Antes de empezar, asegúrese de que dispone de los siguientes parámetros obligatorios:

- `--transit-gateway-metering-policy-id`- El identificador de la política de medición existente
- `--remove-middle-box-attachment-ids`- Uno o más archivos adjuntos IDs para eliminarlos de la política (para eliminar archivos adjuntos)

Para eliminar los adjuntos de middlebox de una política existente mediante la CLI AWS

1. En el siguiente ejemplo, modify-transit-gateway-metering-policy se utiliza para eliminar dos adjuntos específicos de una política de medición existente. El comando elimina solo el adjunto especificado y IDs conserva los adjuntos restantes:

```
aws ec2 modify-transit-gateway-metering-policy \
    --transit-gateway-metering-policy-id tgw-mp-0123456789abcdefg \
    --remove-middle-box-attachment-ids tgw-attach-0456789012345abcd tgw-
attach-0fedcba0987654321
```

2. En el siguiente ejemplo de respuesta, el resultado de JSON muestra la configuración de política actualizada con los adjuntos especificados eliminados y los adjuntos restantes aún activos:

```
{
    "TransitGatewayMeteringPolicy": {
        "TransitGatewayMeteringPolicyId": "tgw-mp-0123456789abcdefg",
        "TransitGatewayId": "tgw-0ecec6433f4bfe55a",
        "MiddleBoxAttachmentIds": [
            "tgw-attach-0bdc681c211bf71f3",
            "tgw-attach-0987654321fedcba0"
        ],
        "State": "available",
        "UpdateEffectiveAt": "2024-09-05T16:00:00.000Z"
    }
}
```

AWS Registros de flujo de Transit Gateway

Los registros de flujo de Transit Gateway son una función de AWS Transit Gateway que le permite capturar información sobre el tráfico IP que entra y sale de sus pasarelas de tránsito. Los datos del registro de flujo se pueden publicar en Amazon CloudWatch Logs, Amazon S3 o Firehose. Una vez creado un registro de flujo, puede recuperarlo y ver sus datos en el destino elegido. Los datos de registro de flujo se recopilan fuera de la ruta del tráfico de red y, por lo tanto, no afectan al rendimiento ni a la latencia de la red. Puede crear o eliminar registros de flujo sin ningún riesgo de impacto en el rendimiento de la red. Los registros de flujo de Transit Gateway capturan información relacionada únicamente con las puertas de enlace de tránsito, tal como se describen en the section called “Registros de flujo de Transit Gateway”. Use registros de flujo de la VPC para capturar información acerca del tráfico IP entrante y saliente de las interfaces de red en su VPC. Consulte Registro del tráfico de IP con registros de flujo de la VPC en la Guía de usuario de la VPC de Amazon para obtener más información.

> **Note**
>
> Para crear un registro de flujo de puerta de enlace de tránsito, debe ser el propietario de la puerta de enlace de tránsito. Si no lo es, el propietario de la puerta de enlace de tránsito debe darle permiso.

Los datos de registro de flujo de una puerta de enlace de tránsito se registran como entradas de registro de flujo, que son eventos de registro que constan de campos que describen el flujo de tráfico. Para obtener más información, consulte Registros de flujo de Transit Gateway.

Para crear un registro de flujo, especifique:

- El recurso para el que desea crear el registro de flujo
- Los destinos a los que desea publicar los datos de registro de flujo

Después de crear un registro de flujo, pueden transcurrir varios minutos hasta que se empiecen a recopilar datos y a publicarse en los destinos elegidos. Los registros de flujo no captan los flujos de registro en tiempo real para sus puertas de enlace de tránsito.

Puede aplicar etiquetas a los registros de flujo. Cada etiqueta está formada por una clave y un valor opcional, ambos definidos por el usuario. Las etiquetas pueden ayudarlo a organizar los registros de flujo, por ejemplo, por finalidad o propietario.

Si ya no necesita un log de flujo, puede eliminarlo. Al eliminar un registro de flujo, se deshabilita el servicio de registro de flujo para el recurso y no se crea ni publica ningún registro de flujo nuevo en CloudWatch Logs o Amazon S3. La eliminación del registro de flujo no elimina ningún registro de registro de flujo o flujo de registro (para CloudWatch Logs) u objeto de archivo de registro (para Amazon S3) existente para una pasarela de tránsito. Para eliminar un flujo de registros existente, utilice la consola de CloudWatch registros. Para eliminar objetos de archivos de registro, utilice la consola de Amazon S3. Tras haber eliminad un log de flujo, puede que se necesiten varios minutos para que se dejen de recopilar los datos. Para obtener más información, consulte Eliminar un registro de registros de flujo de AWS Transit Gateway.

Puede crear registros de flujo para sus pasarelas de tránsito que puedan publicar datos en CloudWatch Logs, Amazon S3 o Amazon Data Firehose. Para obtener más información, consulte los siguientes temas:

- Cree un registro de flujo que se publique en CloudWatch Logs
- Creación de un registro de flujo que se publique en Amazon S3
- Creación de un registro de flujo que se publique en Firehose

Limitaciones

Las siguientes limitaciones se aplican a los registros de flujo de Transit Gateway:

- El tráfico multidifusión no es compatible.
- Las conexiones de Connect no son compatibles. Todos los registros de flujo de Connect figuran en la conexión de transporte y, en consecuencia, deben habilitarse en la puerta de enlace de tránsito y la conexión de transporte de Connect.
- Transit Gateway Flow Logs admite un máximo de 250 suscripciones por recurso y cuenta. Para crear suscripciones adicionales en un recurso que haya alcanzado este límite, primero se deben eliminar las suscripciones existentes.

Registros de flujo de Transit Gateway

Una entrada de registro de flujo representa un flujo de red en su puerta de enlace de tránsito. Cada registro es una cadena con campos separados por espacios. Un registro incluye valores para los distintos componentes del flujo de tráfico, por ejemplo, el origen, el destino y el protocolo.

Al crear un registro de flujo, puede utilizar el formato predeterminado para el registro del registro de flujo o puede especificar un formato personalizado.

Contenido

Formato predeterminado

Con el formato predeterminado, los registros del log de flujo incluyen todos los campos desde la versión 2 hasta la versión 6, en el orden mostrado en la tabla de campos disponibles. No puede personalizar o cambiar el formato predeterminado. Para capturar los campos adicionales o un subconjunto de campos distinto, especifique un formato personalizado.

Formato personalizado

Con un formato personalizado, especifique qué campos se incluyen en los registros de flujo y en qué orden. De este modo, puede crear registros de flujo específicos con arreglo a sus necesidades y omitir los campos que no resulten relevantes. El uso de un formato personalizado puede reducir la necesidad de procesos separados para extraer información específica de registros de flujo publicados. Puede especificar cualquier número de campos de log de flujo disponibles, pero debe especificar al menos uno.

Campos disponibles

La tabla siguiente describe todos los campos disponibles para una entrada de registro de flujo de la puerta de enlace de tránsito. La columna Version (Versión) indica la versión en la que se introdujo el campo.

Al publicar datos de registro de flujo en Amazon S3, el tipo de datos de los campos depende del formato del registro de flujo. Si el formato es texto sin formato, todos los campos son de tipo STRING. Si el formato es Parquet, consulte la tabla de los tipos de datos de campo.

Si un campo no es aplicable o no se pudo calcular para un registro específico, el registro muestra un símbolo “-” en esa entrada. Los campos de metadatos que no provienen directamente del encabezado del paquete son aproximaciones de mejor esfuerzo y sus valores pueden faltar o ser inexactos.

Campo	Descripción	Versión
version	Indica la versión en la que se introdujo el campo. El formato predeterminado incluye todos los campos de la versión 2, en el mismo orden en que aparecen en la tabla. Tipo de datos de Parquet: INT_32	2
resource-type	El tipo de recurso en el que se crea la suscripción. En el caso de los registros de flujo de Transit Gateway, será TransitGateway. Tipo de datos de Parquet: STRING	6
account-id	El Cuenta de AWS ID del propietario de la pasarela de tránsito de origen. Tipo de datos de Parquet: STRING	2
tgw-id	El ID de la puerta de enlace de tránsito para la que se registra el tráfico. Tipo de datos de Parquet: STRING	6
tgw-attachment-id	El ID de la conexión de puerta de enlace de tránsito para el que se registra el tráfico. Tipo de datos de Parquet: STRING	6
tgw-src-vpc-account-id	El Cuenta de AWS ID del tráfico de VPC de origen. Tipo de datos de Parquet: STRING	6

Campo	Descripción	Versión
tgw-dst-vpc-account-id	El Cuenta de AWS ID del tráfico de VPC de destino. Tipo de datos de Parquet: STRING	6
tgw-src-vpc-id	El ID de la VPC de origen para la puerta de enlace de tránsito. Tipo de datos de Parquet: STRING	6
tgw-dst-vpc-id	El ID de la VPC de destino para la puerta de enlace de tránsito. Tipo de datos de Parquet: STRING	6
tgw-src-subnet-id	El ID de la subred para el tráfico de origen de la puerta de enlace de tránsito. Tipo de datos de Parquet: STRING	6
tgw-dst-subnet-id	El ID de la subred para el tráfico de destino de la puerta de enlace de tránsito. Tipo de datos de Parquet: STRING	6
tgw-src-eni	El ID de la conexión de puerta de enlace de tránsito de origen ENI para el flujo. Tipo de datos de Parquet: STRING	6
tgw-dst-eni	El ID de la conexión de puerta de enlace de tránsito de destino ENI para el flujo. Tipo de datos de Parquet: STRING	6
tgw-src-az-id	El ID de la zona de disponibilidad que contiene la puerta de enlace de tránsito para la que se registra el tráfico. Si el tráfico procede de una ubicación secundaria, el registro muestra un símbolo '-' en este campo. Tipo de datos de Parquet: STRING	6

Campo	Descripción	Versión
tgw-dst-az-id	ID de la zona de disponibilidad que contiene la puerta de enlace de tránsito de destino para la que se registra el tráfico. Tipo de datos de Parquet: STRING	6
tgw-pair-attachment-id	En función de la dirección del flujo, este es el ID del accesorio de salida o de entrada del flujo. Tipo de datos de Parquet: STRING	6
srcaddr	La dirección de origen del tráfico entrante. Tipo de datos de Parquet: STRING	2
dstaddr	La dirección de destino del tráfico saliente. Tipo de datos de Parquet: STRING	2
srcport	El puerto de origen del tráfico. Tipo de datos de Parquet: INT_32	2
dstport	El puerto de destino del tráfico. Tipo de datos de Parquet: INT_32	2
protocol	El número de protocolo IANA del tráfico. Para obtener más información, consulte Números de protocolo asignados en internet. Tipo de datos de Parquet: INT_32	2
packets	El número de paquetes transferidos durante el flujo. Tipo de datos de Parquet: INT_64	2
bytes	El número de bytes transferidos durante el flujo. Tipo de datos de Parquet: INT_64	2

Campo	Descripción	Versión
start	Momento, en segundos Unix, en que se recibió el primer paquete del flujo dentro del intervalo de agregación. El tiempo transcurrido puede ser como máximo de 60 segundos una vez que el paquete se ha transmitido o recibido en la puerta de enlace de tránsito. Tipo de datos de Parquet: INT_64	2
end	Momento, en segundos Unix, en que se recibió el último paquete del flujo dentro del intervalo de agregación. El tiempo transcurrido puede ser como máximo de 60 segundos una vez que el paquete se ha transmitido o recibido en la puerta de enlace de tránsito. Tipo de datos de Parquet: INT_64	2
log-status	El estado del registro de flujo: • OK: Los datos se registran normalmente en los destinos elegidos. • NODATA: No hubo tráfico de red hacia o desde la interfaz de red durante el intervalo de agregación. • SKIPDATA: Algunos registros de flujo se omitieron durante el intervalo de agregación. Esto se puede deber a una restricción de capacidad interna, o a un error interno. Tipo de datos de Parquet: STRING	2
type	El tipo de tráfico. Los valores posibles son IPv4 | IPv6 | EFA. Para obtener más información, consulte Elastic Fabric Adapter en la Guía del usuario de Amazon EC2. Tipo de datos de Parquet: STRING	3
packets-lost-no-route	Los paquetes se perdieron debido a que no se especificó ninguna ruta. Tipo de datos de Parquet: INT_64	6

Campo	Descripción	Versión
packets-lost-blackhole	Los paquetes se perdieron debido a un agujero negro. Tipo de datos de Parquet: INT_64	6
packets-lost-mtu-exceeded	Los paquetes perdidos debido a que el tamaño excede la MTU. Tipo de datos de Parquet: INT_64	6
packets-lost-ttl-expired	Los paquetes perdidos debido a la expiración del tiempo de vida. Tipo de datos de Parquet: INT_64	6

Campo	Descripción	Versión
tcp-flags	El valor de máscara de bits de las siguientes marcas TCP: • FIN: 1 • SYN: 2 • RST: 4 • PSH: 8 • ACK: 16 • SYN-ACK — 18 • URG: 32 **Important** Cuando una entrada de registro de flujo consta solo de paquetes ACK, el valor de marca es 0, no 16. Para obtener información general sobre marcadores TCP (como el significado de marcadores como FIN, SYN y ACK), consulte TCP segment structure (Estructura de segmentos TCP) en Wikipedia. Los indicadores TCP pueden estar OR-ed durante el intervalo de agregación. En el caso de las conexiones cortas, los indicadores pueden estar configurados en la misma línea del registro de flujo, por ejemplo, 19 para FIN SYN-ACK y 3 para SYN y FIN. Tipo de datos de Parquet: INT_32	3
region	La región que contiene la puerta de enlace de tránsito en la que se registra el tráfico. Tipo de datos de Parquet: STRING	4

Campo	Descripción	Versión
flow-direction	La dirección del flujo con respecto a la pasarela de tránsito. Los valores posibles son: ingress | egress. Tipo de datos de Parquet: STRING	5
pkt-src-aws-service	El nombre del subconjunto de rangos de direcciones IP srcaddr si la dirección IP de origen es para un AWS servicio. Los valores posibles son: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Tipo de datos de Parquet: STRING	5
pkt-dst-aws-service	El nombre del subconjunto de rangos de direcciones IP del dstaddr campo, si la dirección IP de destino es para un AWS servicio. Para obtener una lista de posibles valores, consulte el campo pkt-src-aws-service. Tipo de datos de Parquet: STRING	5

Controlar el uso de los registros de flujo

De forma predeterminada, los usuarios no tienen permiso para trabajar con registros de flujo. Puede crear una política de usuarios de que conceda permisos a los usuarios para crear, describir y eliminar registros de flujo. Para obtener más información, consulte Concesión a los usuarios de IAM de los permisos necesarios para los recursos de Amazon EC2 en la Referencia de la API de Amazon EC2.

A continuación se muestra una política de ejemplo que concede a los usuarios permisos completos para crear, describir y eliminar logs de flujo.

JSON

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

Se requiere alguna configuración adicional de roles y permisos de IAM, dependiendo de si publica en CloudWatch Logs o Amazon S3. Para obtener más información, consulte AWS Transit Gateway Flow registra registros en Amazon CloudWatch Logs y AWS Registros de flujo de Transit Gateway en Amazon S3.

Precios de los registros de flujo de la puerta de enlace de tránsito

Se aplican cargos por almacenamiento e ingesta de datos para registros distribuidos cuando publica registros de flujo de puerta de enlace. Para obtener más información sobre los precios de la publicación de registros vendidos, abre Amazon CloudWatch Pricing y, a continuación, en la capa de pago, selecciona Logs y busca Vended Logs.

Crear o actualizar un rol de IAM para los registros de flujo de AWS Transit Gateway

Puede actualizar un rol existente o usar el siguiente procedimiento para crear un nuevo rol para usarlo con los registros de flujo mediante la AWS Identity and Access Management consola.

Para crear un rol de IAM para registros de flujo

1. Abra la consola de IAM en https://console.aws.amazon.com/iam/.

2. En el panel de navegación, elija Roles, Create role.
3. En Select type of trusted entity (Seleccionar tipo de entidad de confianza), elija AWS service (Servicio de AWS). En Use case (Caso de uso), elija EC2. Elija Next (Siguiente).
4. En la página Attach permissions policies (Asociar políticas de permisos), elija Next: Review (Siguiente: Revisar). Elija Siguiente.
5. En la página Nombrar, revisar y crear, especifique un nombre para el rol y, de manera opcional, especifique una descripción. Elija Crear rol.
6. Seleccione el nombre de su rol. Para Add permissions (Agregar permisos), elija Create Inline Policy (Crear política insertada) y, luego, elija la pestaña JSON.
7. Copie la primera política de Funciones de IAM para publicar los registros de flujo en Logs CloudWatch y péguela en la ventana. Elija Review policy (Revisar política).
8. Escriba un nombre para la política y elija Create policy (Crear política).
9. Seleccione el nombre de su función. En Trust relationships (Relaciones de confianza), seleccione Edit trust relationship (Editar relación de confianza). En el documento de la política existente, cambie el servicio de `ec2.amazonaws.com` a `vpc-flow-logs.amazonaws.com`. Elija Update Trust Policy.
10. En la página Summary (Resumen), tome nota del ARN de la función. Necesita este ARN para crear su propio log de flujo.

AWS Transit Gateway Flow registra registros en Amazon CloudWatch Logs

Los registros de flujo pueden publicar los datos del registro de flujo directamente en Amazon CloudWatch.

Cuando se publican en CloudWatch Logs, los datos del registro de flujo se publican en un grupo de registros y cada pasarela de tránsito tiene un flujo de registro único en el grupo de registros. Los flujos de registro contienen registros de flujo. Puede crear varios registros de flujo que publiquen datos en el mismo grupo de registro. Si la misma puerta de enlace de tránsito está presente en uno o varios registros de flujo en el mismo grupo de registro, tendrá un flujo de registro combinado. Si ha especificado que un registro de flujo debe capturar el tráfico rechazado y otro registro de flujo debe capturar el tráfico aceptado, el flujo de registros combinado capturará todo el tráfico.

Al publicar los registros de flujo en Logs, se cobran cargos por la ingesta y el archivado de datos por los registros vendidos. CloudWatch Para obtener más información, consulta los CloudWatch precios de Amazon.

En CloudWatch los registros, el campo de fecha y hora corresponde a la hora de inicio que se captura en el registro del flujo. El campo IngestionTime proporciona la fecha y la hora en que Logs recibió el registro del registro de flujo. CloudWatch La marca de tiempo es posterior a la hora de finalización capturada en la entrada de registro de flujo.

Para obtener más información sobre CloudWatch los registros, consulte Logs sent to CloudWatch Logs en la Guía del usuario de Amazon CloudWatch Logs.

Contenido

Funciones de IAM para publicar los registros de flujo en Logs CloudWatch

La función de IAM asociada al registro de flujo debe tener permisos suficientes para publicar los registros de flujo en el grupo de registros especificado en CloudWatch Logs. El rol de IAM debe pertenecerle. Cuenta de AWS

La política de IAM asociada al rol de IAM debe incluir al menos los siguientes permisos.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
```

```
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
    }
  ]
}
```

Asegúrese también de que el rol tiene una relación de confianza que permite al servicio de registros de flujo asumir ese rol.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Le recomendamos que utilice las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse contra el problema del suplente confuso. Por ejemplo, podría agregar el siguiente bloque de condición a la política de confianza anterior. La cuenta fuente es la propietaria del registro de flujo y el ARN fuente es el ARN del registro de flujo. Si no conoce el ID del registro de flujo, puede reemplazar esa parte del ARN por un comodín (*) y, a continuación, actualizar la política después de crear el registro de flujo.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
```

```
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Permisos para que los usuarios de IAM pasen un rol

Los usuarios también deben tener permisos para utilizar la acción `iam:PassRole` para el rol de IAM que está asociado con registro de flujo.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
        }
    ]
}
```

Cree un registro de registros de flujo de AWS Transit Gateway que se publique en Amazon CloudWatch Logs

Puede crear entradas de registro de flujo para las puertas de enlace de tránsito. Si realiza estos pasos como usuario de IAM, asegúrese de que tiene permisos para usar la acción `iam:PassRole`. Para obtener más información, consulte Permisos para que los usuarios de IAM pasen un rol.

Puede crear un registro de CloudWatch flujo de Amazon mediante la consola de Amazon VPC o la CLI AWS .

Para crear un registro de flujo de la puerta de enlace de tránsito mediante la consola

1. Inicie sesión en la consola de Amazon VPC Consola de administración de AWS y ábrala en. https://console.aws.amazon.com/vpc/

2. En el panel de navegación, seleccione Transit gateways (Puertas de enlace de tránsito).
3. Seleccione las casillas de verificación de una o más puertas de enlace de tránsito y elija Acciones, Crear registro de flujo.
4. En Destino, selecciona Enviar a CloudWatch registros.
5. Para Grupo de registro de destino, elija el nombre del grupo de registro de destino que ha creado.

   > **Note**
   >
   > Si el grupo de registro de destino aún no existe, si introduce un nombre nuevo en este campo, se creará un nuevo grupo de registro de destino.

6. Para el rol de IAM, especifique el nombre del rol que tiene permisos para publicar registros en CloudWatch Logs.
7. Para Log record format (Formato de registro de registro), seleccione el formato para el registro de flujo.
   - Para utilizar el formato predeterminado, elija Formato predeterminado de AWS .
   - Para utilizar un formato personalizado, elija Custom format (Formato personalizado) y, a continuación, seleccione campos de Log format (Formato de registro).
8. (Opcional) Elija Add new tag (Agregar etiqueta nueva) para aplicar etiquetas al registro de flujo.
9. Elija Create flow log (Crear registro de flujo).

Para crear un registro de flujo mediante la línea de comandos

Utilice uno de los siguientes comandos.

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

En el siguiente AWS CLI ejemplo, se crea un registro de flujo que captura la información de la pasarela de tránsito. Los registros de flujo se envían a un grupo de CloudWatch registros en los registros denominados`my-flow-logs`, en la cuenta 123456789101, con la función de IAM. `publishFlowLogs`

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-1a2b3c4d --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Ver los registros de flujos de AWS Transit Gateway en Amazon CloudWatch

Puede ver los registros de registro de flujo mediante la consola CloudWatch Logs o la consola Amazon S3, según el tipo de destino elegido. Es posible que, después de crear su registro de flujo, se necesiten unos minutos para que se encuentre visible en la consola.

Para ver los registros de registro de flujo publicados en CloudWatch Logs

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Logs (Registros) y seleccione el grupo de registro que contiene el registro de flujo. Aparecerá una lista de flujos de registros para cada puerta de enlace de tránsito.
3. Seleccione el flujo de registro que contiene el ID de la puerta de enlace de tránsito para la que desea ver los registros de log de flujo. Para obtener más información, consulte Registros de flujo de Transit Gateway.

Procesa los registros de flujos de AWS Transit Gateway en Amazon CloudWatch Logs

Puede trabajar con los registros de flujo del mismo modo que lo haría con cualquier otro evento de registro recopilado por CloudWatch Logs. Para obtener más información sobre la supervisión de los filtros de métricas y datos de registro, consulte Creación de métricas a partir de eventos de registro mediante filtros en la Guía del CloudWatch usuario de Amazon.

Ejemplo: crear un filtro CloudWatch métrico y una alarma para un registro de flujo

En este ejemplo, tiene un log de flujo para `tgw-123abc456bca`. Desea crear una alarma que le avise si ha habido 10 o más intentos rechazados para conectar con su instancia a través del puerto TCP 22 (SSH) en un periodo de 1 hora. En primer lugar, debe crear un filtro de métrica que coincida con el patrón de tráfico para el que va a crear la alarma. A continuación, puede crear una alarma para el filtro de métrica.

Para crear un filtro de métrico para el tráfico SSH rechazado y una alarma para el filtro

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Logs (Registros), Log groups (Grupos de registro).
3. Marque la casilla de verificación del grupo de registro y, a continuación, seleccione Acciones, Crear filtro de métricas.
4. En Filter Pattern (Patrón de filtro), escriba lo siguiente.

```
[version, resource_type, account_id,tgw_id="tgw-123abc456bca”, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= "10.0.0.1", dstaddr,
 srcport=“80”, dstport, protocol=“6”, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

5. En Select Log Data to Test (Seleccionar datos de registro para prueba), seleccione el flujo de registro para la puerta de enlace de tránsito. (Opcional) Para ver las líneas de los datos de registro que concuerdan con el patrón de filtro, elija Test Pattern (Probar patrón). Cuando esté preparado para continuar, seleccione Next (Siguiente).
6. Ingrese un nombre de filtro, un espacio de nombres de métrica y un nombre de métrica. Establezca el valor de la métrica en **1**. Cuando haya terminado, elija Next (Siguiente) y, luego, elija Create metric filter (Crear filtro de métricas).
7. En el panel de navegación, elija Alarms (Alarmas), Create Alarm (Crear alarma).
8. Elija Crear alarma.
9. Elija el espacio de nombres para el filtro de métricas que ha creado.

   Puede que la nueva métrica tarde unos minutos en mostrarse en la consola.
10. Seleccione el nombre de métrica que ha creado y elija Next (Siguiente).
11. Configure la alarma como se indica a continuación y, luego, elija Next (Siguiente):

    - En Statistic (Estadística), elija Sum (Suma). Asegura que esté capturando el número total de puntos de datos para el período especificado.
    - En Period (Período), seleccione 1 Hour (1 hora).
    - En Whenever (Cada vez que), elija Greater/Equal (Mayor o igual) e ingrese **10** para el umbral.

- En Additional configuration (Configuración adicional), Datapoints to alarm (Puntos de datos para alarma), deje el valor predeterminado **1**.

12. Para Notification (Notificación), seleccione un tema de SNS existente o elija Create new topic (Crear tema nuevo) para crear uno nuevo. Elija Siguiente.
13. Ingrese un nombre y una descripción para la alarma y, a continuación, elija Next (Siguiente).
14. Cuando haya terminado de configurar la alarma, elija Create alarm (Crear alarma).

AWS Registros de flujo de Transit Gateway en Amazon S3

Los registros de flujo pueden publicar datos de registros de flujo en Amazon S3.

Al publicar en Amazon S3, los datos de registro de flujo se publican en un bucket de Amazon S3 existente que especifique. Las entradas de registros de flujo de todas las puertas de enlace de tránsito monitoreadas se publican en una serie de objetos de archivos de registro que se almacenan en el bucket.

Al publicar los registros de flujo en Amazon S3, los cargos Amazon CloudWatch por ingesta y archivado de datos se aplican a los registros vendidos. Para obtener más información sobre CloudWatch los precios de los registros vendidos, abre Amazon CloudWatch Pricing, selecciona Logs y, a continuación, busca Vended Logs.

Para crear un bucket de Amazon S3 y utilizarlo con los registros de flujo, consulte Creación de un bucket en la Guía del usuario de Amazon S3.

Para obtener más información acerca del registro de varias cuentas, consulte Registro central en la Biblioteca de soluciones de AWS .

Para obtener más información sobre CloudWatch los registros, consulte Registros enviados a Amazon S3 en la Guía del usuario de Amazon CloudWatch Logs.

Contenido

- Cree el rol de cuenta de origen de AWS Transit Gateway Flow Logs para Amazon S3
- Cree un registro de registros de flujo de AWS Transit Gateway que se publique en Amazon S3
- Ver los registros de flujos de AWS Transit Gateway en Amazon S3
- Registros de registros de flujo de AWS Transit Gateway procesados en Amazon S3

Archivos de registro de flujo

VPC Flow Logs es una función que recopila colecciones de entradas de registros de flujo, las consolidan en archivos de registro y, a continuación, publican los archivos de registro en el bucket de Amazon S3 en intervalos de cinco minutos. Cada archivo de registro contiene registros de flujo del tráfico IP registrado en los cinco minutos anteriores.

El tamaño de archivo máximo de un archivo log es de 75 MB. Si el archivo log alcanza el límite de tamaño de archivo en el periodo de cinco minutos, el log de flujo deja de añadirle registros de logs de flujo. A continuación, publica el registro de flujo en el bucket de Amazon S3 y crea un nuevo archivo de registro.

En Amazon S3, el campo Last modified (Última modificación) del archivo de registro de flujo indica la fecha y la hora en que el archivo se cargó en el bucket de Amazon S3. Este valor es posterior a la marca temporal del nombre de archivo y difiere en la cantidad de tiempo invertido en cargar el archivo en el bucket de Amazon S3.

Formato de archivo de registro

Puede especificar uno de los siguientes formatos para los archivos de registro. Cada archivo se comprime en un único archivo Gzip.

- Texto: Texto sin formato. Este es el formato predeterminado.
- Parquet: Apache Parquet es un formato de datos columnar. Las consultas sobre los datos en formato Parquet son de 10 a 100 veces más rápidas en comparación con las consultas de datos en texto sin formato. Los datos en formato Parquet con compresión Gzip ocupan un 20 por ciento menos de espacio de almacenamiento que el texto sin formato con compresión Gzip.

Opciones de archivo de registro

Puede especificar las siguientes opciones:

- Prefijos de S3 compatibles con Hive: Habilite los prefijos compatibles con Hive en lugar de importar las particiones a las herramientas compatibles con Hive. Antes de ejecutar las consultas, utilice el comando MSCK REPAIR TABLE.
- Particiones por horas: Si tiene un gran volumen de registros y, por lo general, orienta las consultas a una hora en específico, puede obtener resultados más rápidos y ahorrar en costos de consulta si particiona los registros por hora.

Estructura del bucket de S3 del archivo de registro

Los archivos de registro se guardan en el bucket de Amazon S3 especificado con una estructura de carpetas basada en el ID del registro de flujo, la Región, la fecha en que se crearon y en las opciones de destino.

De forma predeterminada, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Si habilita los prefijos de S3 compatibles con Hive, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-
region=region/year=year/month=month/day=day/
```

Si habilita particiones por hora, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Si habilita particiones compatibles con Hive y particiona el registro de flujo por hora, los archivos se entregan en la siguiente ubicación.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/service=vpcflowlogs/aws-
region=region/year=year/month=month/day=day/hour=hour/
```

Nombre de archivo de registro

El nombre de archivo de un archivo de registro se basa en el ID del registro de flujo, la Región y en la fecha y hora de creación. Los nombres de archivo utilizan el formato siguiente.

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

A continuación, se muestra un ejemplo de un archivo de registros para un registro de flujo que la Cuenta de AWS 123456789012 ha creado para un recurso en la Región us-east-1, el June 20, 2018 a las 16:20 UTC. El archivo contiene las colecciones de datos del registro de flujo con una hora de finalización entre las 16:20:00 y las 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Política de IAM para entidades principales de IAM que publican registros de flujo en Amazon S3

La entidad principal de IAM que crea el registro de flujo debe tener los siguientes permisos, que son necesarios para publicar registros de flujo en el bucket de Amazon S3 de destino.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
        ],
      "Resource": "*"
    }
  ]
}
```

Permisos del bucket de Amazon S3 para registros de flujo

De forma predeterminada, los buckets de Amazon S3 y los objetos que contienen son privados. Solo el propietario del bucket puede tener acceso al bucket y a los objetos almacenados en él. Sin embargo, el propietario del bucket puede conceder acceso a otros recursos y usuarios escribiendo una política de acceso.

Si el usuario que crea el registro de flujo es el propietario del bucket y tiene permisos `PutBucketPolicy` y `GetBucketPolicy` para el bucket, adjuntamos de forma automática la

siguiente política al bucket. Esta nueva política generada automáticamente se adjunta a la política original.

De otra manera, el propietario del bucket debe agregar esta política al bucket, al especificar el ID de Cuenta de AWS del creador del registro de flujo o fallará la creación del registro de flujo. Para obtener más información, consulte Políticas de bucket en la Guía del usuario de Amazon Simple Storage Service.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::bucket_name/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
                }
            }
        }
    ]
}
```

El ARN que especifique *my-s3-arn* depende de si utiliza prefijos S3 compatibles con HIVE.

- Prefijos predeterminados

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- Prefijos de S3 compatibles con HIVE

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Como práctica recomendada, le recomendamos que conceda estos permisos al director del servicio de entrega de registros en lugar de a una persona. Cuenta de AWS ARNs También es una práctica recomendada utilizar las claves de condición `aws:SourceAccount` y `aws:SourceArn` para protegerse del problema del suplente confuso. La cuenta fuente es la propietaria del registro de flujo y el ARN fuente es el ARN comodín (*) del servicio de registros.

Política de clave requerida para el uso con SSE-KMS

Para proteger los datos del bucket de Amazon S3, habilite el cifrado del lado del servidor con las claves administradas de Amazon S3 (SSE-S3) o con el cifrado del lado del servidor con claves de KMS (SSE-KMS). Para obtener más información, consulte Protección de datos mediante cifrado del lado del servidor en la Guía del usuario de Amazon S3.

Con SSE-KMS, puede usar una clave administrada o una clave AWS administrada por el cliente. Con una clave AWS gestionada, no puede utilizar la entrega entre cuentas. Los registros de flujo se entregan desde la cuenta de entrega de registros, por lo que debe conceder acceso para la entrega entre cuentas. Para conceder acceso de cuentas cruzadas al bucket de S3, utilice una clave administrado por el cliente y especifique el nombre de recurso de Amazon (ARN) de la clave

administrada por el cliente cuando habilite el cifrado del bucket. Para obtener más información, consulte Especificación del cifrado del lado del servidor con AWS KMS en la Guía del usuario de Amazon S3.

Cuando utilice SSE-KMS con una clave administrado por el cliente, debe agregar lo siguiente a la política de clave destinada a su clave (no la política de bucket para el bucket de S3), de modo que VPC Flow Logs pueda realizar registros en el bucket de S3.

> **Note**
>
> El uso de S3 Bucket Keys le permite ahorrar en AWS Key Management Service (AWS KMS) costes de solicitud al reducir las AWS KMS solicitudes a operaciones de cifrado y descifrado mediante el uso de una clave de nivel de depósito. GenerateDataKey Por diseño, las solicitudes posteriores que utilizan esta clave de nivel de depósito no generan solicitudes de AWS KMS API ni validan el acceso con arreglo a la política de claves. AWS KMS

```
{
    "Sid": "Allow Transit Gateway Flow Logs to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
   "Action": [
       "kms:Encrypt",
       "kms:Decrypt",
       "kms:ReEncrypt*",
       "kms:GenerateDataKey*",
       "kms:DescribeKey"
    ],
    "Resource": "*"
}
```

Permisos de archivos de registro de Amazon S3

Además de las políticas de bucket requeridas, Amazon S3 usa listas de control de acceso (ACLs) para administrar el acceso a los archivos de registro creados por un registro de flujo. De forma predeterminada, el propietario del bucket tiene los permisos `FULL_CONTROL` en cada archivo log.

El propietario de la entrega de logs, si es diferente del propietario del bucket, no tiene permisos. La cuenta de entrega de registros tiene los permisos `READ` y `WRITE`. Para obtener más información, consulte Información general de la Lista de control de acceso (ACL) en la Guía del usuario de Amazon Simple Storage Service.

Cree el rol de cuenta de origen de AWS Transit Gateway Flow Logs para Amazon S3

Desde la cuenta de origen, cree el rol de origen en la AWS Identity and Access Management consola.

Para crear el rol de la cuenta de origen

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create policy (Crear política), haga lo siguiente:
    1. Elija JSON.
    2. Reemplace el contenido de esta ventana por la política de permisos que aparece al principio de esta sección.
    3. Elija Next: Tags (Siguiente: Etiquetas) y Next: Review (Siguiente: Revisar).
    4. Introduzca un nombre para su política y una descripción opcional y, a continuación, elija Create policy (Crear política).
5. Seleccione Roles en el panel de navegación.
6. Elija Create role (Crear rol).
7. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada). En Custom trust policy (Política de confianza personalizada), reemplace `"Principal": {},` con lo siguiente, lo cual especifica el servicio de entrega de registros. Elija Siguiente.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. En la página Add permissions (Agregar permisos), seleccione la casilla de verificación de la política que creó anteriormente en este procedimiento y luego elija Next (Siguiente).
9. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción.
10. Elija Create role (Crear rol).

Cree un registro de registros de flujo de AWS Transit Gateway que se publique en Amazon S3

Después de haber creado y configurado el bucket de Amazon S3, puede crear registros de flujo para las puertas de enlace de tránsito. Puede utilizar la consola de Amazon VPC o la CLI de AWS para crear un registro de flujo de Amazon S3.

Para crear un registro de flujo de puerta de enlace de tránsito que publica en Amazon S3 mediante la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway (Puerta de enlace de tránsito) o Transit gateway attachments (Conexión de la puerta de enlace de tránsito).
3. Seleccione las casillas de verificación de una o más puertas de enlace de tránsito o conexiones de puerta de enlace de tránsito.
4. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).
5. Establezca la configuración del registro de flujo. Para obtener más información, consulte To configure flow log settings (Configuración del registro de flujo).

Configuración del registro de flujo mediante la consola

1. En Destination (Destino), elija Send to an Amazon S3 bucket (Enviar a un bucket de S3).
2. En S3 bucket ARN (ARN de bucket de S3), especifique el nombre de recurso de Amazon (ARN) de un bucket de Amazon S3 existente. Si lo desea, puede incluir una subcarpeta. Por ejemplo, para especificar una subcarpeta llamada `my-logs` de un bucket denominado `my-bucket`, utilice el siguiente ARN:

   ```
   arn:aws::s3:::my-bucket/my-logs/
   ```

El bucket no puede utilizar `AWSLogs` como nombre de subcarpeta, ya que se trata de un término reservado.

Si posee el bucket, crearemos automáticamente una política de recursos y la asociaremos al bucket. Para obtener más información, consulte Permisos del bucket de Amazon S3 para registros de flujo.

3. Para Log record format (Formato de registro), seleccione el formato para el registro de flujo.
   - Para utilizar el formato de registro predeterminado del registro de flujo, elija Formato predeterminado de AWS .
   - Para crear un formato personalizado, seleccione Formato personalizado. En Log format (Formato de log), elija los campos que desea incluir en el registro de flujo.
4. Para Log file format (Formato de archivo de registro), especifique el formato del archivo de registro.
   - Text (Texto): Texto sin formato. Este es el formato predeterminado.
   - Parquet: Apache Parquet es un formato de datos columnar. Las consultas sobre los datos en formato Parquet son de 10 a 100 veces más rápidas en comparación con las consultas de datos en texto sin formato. Los datos en formato Parquet con compresión Gzip ocupan un 20 por ciento menos de espacio de almacenamiento que el texto sin formato con compresión Gzip.
5. (Opcional) Para utilizar prefijos de S3 compatibles con Hive, elija Hive-compatible S3 prefix (Prefijo de S3 compatible con Hive) y, a continuación, Enable (Habilitar).
6. (Opcional) Para particionar los registros de flujo por hora, elija Every 1 hour (60 mins) (Cada 1 hora [60 minutos]).
7. (Opcional) Para agregar una etiqueta al registro de flujo, elija Add new tag (Añadir nueva etiqueta) y especifique la clave y el valor de etiqueta.
8. Elija Create flow log (Crear registro de flujo).

Para crear un registro de flujo que publica en Amazon S3 mediante una herramienta de línea de comandos

Utilice uno de los siguientes comandos.

- create-flow-logs (AWS CLI)

- New-EC2FlowLog (AWS Tools for Windows PowerShell)

El siguiente AWS CLI ejemplo crea un registro de flujo que captura todo el tráfico de la puerta de enlace de tránsito para la VPC `tgw-00112233344556677` y entrega los registros de flujo a un bucket de Amazon S3 llamado. `flow-log-bucket` El parámetro `--log-format` especifica un formato personalizado para las entradas de registros de flujo.

```
aws ec2 create-flow-logs --resource-type TransitGateway --resource-ids
 tgw-00112233344556677 --log-destination-type s3 --log-destination arn:aws:s3:::flow-
log-bucket/my-custom-flow-logs/'
```

Ver los registros de flujos de AWS Transit Gateway en Amazon S3

Para consultar las entradas de registro de flujo publicadas en Amazon S3

1. Abra la consola de Amazon S3 en https://console.aws.amazon.com/s3/.
2. En Bucket name (Nombre del bucket), seleccione el bucket en el que se van a publicar los logs de flujo.
3. En Nombre, marque la casilla de verificación ubicada junto al archivo de registro. En el panel de información general del objeto, elija Download (Descargar).

Registros de registros de flujo de AWS Transit Gateway procesados en Amazon S3

Los archivos log están comprimidos. Si abre los archivos de registro con la consola de Amazon S3, se descomprimen y se muestran las entradas de registro de flujo. Si descarga los archivos, debe descomprimirlos para ver los registros de flujo.

AWS Transit Gateway, registros de flujo en Amazon Data Firehose

Temas

- Roles de IAM para la entrega entre cuentas
- Cree el rol de cuenta de origen de AWS Transit Gateway Flow Logs para Amazon Data Firehose
- Cree el rol de cuenta de destino de AWS Transit Gateway Flow Logs para Amazon Data Firehose

- Cree un registro de registros de flujo de AWS Transit Gateway que se publique en Amazon Data Firehose

Los registros de flujo pueden publicar datos de registros de flujo directamente en Firehose. Puede optar por publicar los registros de flujo en la misma cuenta que el monitor de recursos o en una cuenta diferente.

Requisitos previos

Al publicarlos en Firehose, los datos del registro de flujo se publican en un flujo de entrega de Firehose en formato de texto sin formato. Primero debe haber creado un flujo de entrega de Firehose. Para conocer los pasos para crear un flujo de entrega, consulte Creación de un flujo de entrega de Amazon Data Firehose en la Guía para desarrolladores de Amazon Data Firehose.

Precios

Se aplican los cargos estándar de ingesta y entrega. Para obtener más información, abre Amazon CloudWatch Pricing, selecciona Logs y busca Vended Logs.

Roles de IAM para la entrega entre cuentas

Al publicar en Kinesis Data Firehose, puede elegir un flujo de entrega que esté en la misma cuenta que el recurso que se va a supervisar (la cuenta de origen) o en una cuenta diferente (la cuenta de destino). Para habilitar la entrega entre cuentas de los registros de flujo a Firehose, debe crear un rol de IAM en la cuenta de origen y un rol de IAM en la cuenta de destino.

Roles

- Rol de cuenta de origen
- Rol de cuenta de destino

Rol de cuenta de origen

En la cuenta de origen, cree un rol que conceda los siguientes permisos. En este ejemplo, el nombre del rol es `mySourceRole`, pero puede elegir un nombre diferente para este rol. La última instrucción permite que el rol de la cuenta de destino asuma este rol. Las instrucciones de condición garantizan que esta función se pase solo al servicio de entrega de registros y solo al supervisar el recurso especificado. Cuando crees tu política, especifica las VPCs interfaces de red o subredes que vas a monitorear con la clave de condición. `iam:AssociatedResourceARN`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::111122223333:role/mySourceRole",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "delivery.logs.amazonaws.com"
                },
                "StringLike": {
                    "iam:AssociatedResourceARN": [
                        "arn:aws:ec2:us-east-1:source-account:transit-gateway/
tgw-0fb8421e2da853bf"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery",
                "logs:ListLogDeliveries",
                "logs:GetLogDelivery"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
        }
    ]
}
```

Asegúrese de que este rol tenga la siguiente política de confianza, la cual permite que el servicio de entrega de registros asuma el rol.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Rol de cuenta de destino

En la cuenta de destino, cree un rol con un nombre que comience por. AWSLogDeliveryFirehoseCrossAccountRole El rol debe otorgar los siguientes permisos.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
          "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

Asegúrese de que este rol tenga la siguiente política de confianza, la cual permite que el rol que creó en la cuenta de origen asuma este rol.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/mySourceRole"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Cree el rol de cuenta de origen de AWS Transit Gateway Flow Logs para Amazon Data Firehose

Desde la cuenta de origen, cree el rol de origen en la AWS Identity and Access Management consola.

Para crear el rol de la cuenta de origen

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create policy (Crear política), haga lo siguiente:
    1. Elija JSON.
    2. Reemplace el contenido de esta ventana por la política de permisos que aparece al principio de esta sección.
    3. Elija Next: Tags (Siguiente: Etiquetas) y Next: Review (Siguiente: Revisar).

4. Introduzca un nombre para su política y una descripción opcional y, a continuación, elija Create policy (Crear política).
5. Seleccione Roles en el panel de navegación.
6. Elija Create role (Crear rol).
7. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada). En Custom trust policy (Política de confianza personalizada), reemplace `"Principal": {},` con lo siguiente, lo cual especifica el servicio de entrega de registros. Elija Siguiente.

```
"Principal": {
   "Service": "delivery.logs.amazonaws.com"
},
```

8. En la página Add permissions (Agregar permisos), seleccione la casilla de verificación de la política que creó anteriormente en este procedimiento y luego elija Next (Siguiente).
9. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción.
10. Elija Create role (Crear rol).

Cree el rol de cuenta de destino de AWS Transit Gateway Flow Logs para Amazon Data Firehose

Desde la cuenta de destino, cree el rol de destino en la AWS Identity and Access Management consola.

Para crear el rol de cuenta de destino

1. Inicie sesión en la consola de IAM Consola de administración de AWS y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación, seleccione Políticas.
3. Elija Create Policy (Crear política).
4. En la página Create policy (Crear política), haga lo siguiente:

    1. Elija JSON.
    2. Reemplace el contenido de esta ventana por la política de permisos que aparece al principio de esta sección.
    3. Elija Next: Tags (Siguiente: Etiquetas) y Next: Review (Siguiente: Revisar).

4. Introduzca un nombre para la política que empiece por y AWSLogDeliveryFirehoseCrossAccountRole, a continuación, seleccione Crear política.
5. Seleccione Roles en el panel de navegación.
6. Elija Create role (Crear rol).
7. En Trusted entity type (Tipo de entidad de confianza), elija Custom trust policy (Política de confianza personalizada). En Custom trust policy (Política de confianza personalizada), reemplace `"Principal": {},` con lo siguiente, lo cual especifica el servicio de entrega de registros. Elija Siguiente.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. En la página Add permissions (Agregar permisos), seleccione la casilla de verificación de la política que creó anteriormente en este procedimiento y luego elija Next (Siguiente).
9. Ingrese un nombre para el rol y, opcionalmente, especifique una descripción.
10. Elija Create role (Crear rol).

Cree un registro de registros de flujo de AWS Transit Gateway que se publique en Amazon Data Firehose

Cree un registro de flujo de Transit Gateway que publique en Amazon Data Firehose. Antes de que cree el registro de flujo, asegúrese de haber configurado los roles de IAM de las cuentas de origen y destino para la entrega entre cuentas y de haber creado el flujo de entrega de Firehose. Para obtener más información, consulte Registros de flujo en Amazon Data Firehose. Puede crear un registro de flujo de Firehose mediante la consola de Amazon VPC o la CLI. AWS

Para crear un registro de flujo de puerta de enlace de tránsito que publica en Firehose desde la consola

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway (Puerta de enlace de tránsito) o Transit gateway attachments (Conexión de la puerta de enlace de tránsito).
3. Seleccione las casillas de verificación de una o más puertas de enlace de tránsito o conexiones de puerta de enlace de tránsito.
4. Seleccione Actions (Acciones) y, a continuación, Create flow log (Crear registro de flujo).

5. En Destination (Destino) elija Enviar a Firehose Delivery System (Sistema de entrega de Firehose).
6. En Firehose Delivery Stream ARN (ARN de flujo de entrega de Firehose), elija el ARN de un flujo de entrega que haya creado en el que se publicará el registro de flujo.
7. Para Log record format (Formato de registro), seleccione el formato para el registro de flujo.
   - Para utilizar el formato de registro predeterminado del registro de flujo, elija Formato predeterminado de AWS .
   - Para crear un formato personalizado, seleccione Formato personalizado. En Log format (Formato de log), elija los campos que desea incluir en el registro de flujo.
8. (Opcional) Para agregar una etiqueta al registro de flujo, elija Add new tag (Agregar nueva etiqueta) y especifique la clave y el valor de etiqueta.
9. Elija Create flow log (Crear registro de flujo).

Para crear un registro de flujo que publica en Firehose desde la línea de comandos

Utilice uno de los siguientes comandos:

- create-flow-logs (CLI)AWS
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

El siguiente ejemplo de AWS CLI crea un registro de flujo que captura la información de la pasarela de tránsito y entrega el registro de flujo al flujo de entrega de Firehose especificado.

```
aws ec2 create-flow-logs \
                --resource-type TransitGateway \
                --resource-ids tgw-1a2b3c4d \
                --log-destination-type kinesis-data-firehose \
                --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

El siguiente ejemplo de AWS CLI crea un registro de flujo que captura la información de la pasarela de tránsito y entrega el registro de flujo a un flujo de entrega de Firehose diferente de la cuenta de origen.

```
aws ec2 create-flow-logs  \
  --resource-type TransitGateway \
```

```
  --resource-ids gw-1a2b3c4d \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Cree y gestione los registros de flujo de AWS Transit Gateway mediante APIs o la CLI

Puede utilizar la línea de comandos para realizar las tareas descritas en esta página.

Al usar el create-flow-logscomando, se aplican las siguientes limitaciones:

- `--resource-ids` tiene una restricción máxima de 25 tipos de recursos `TransitGateway` o `TransitGatewayAttachment`.
- `--traffic-type` no es un campo obligatorio de forma predeterminada. Se devuelve un error si lo proporciona para los tipos de recursos de puerta de enlace de tránsito. Este límite se aplica únicamente a los tipos de recurso de puerta de enlace de tránsito.
- `--max-aggregation-interval` tiene un valor predeterminado de `60` y es el único valor aceptado para los tipos de recursos de puerta de enlace de tránsito. Se devuelve un error si intenta pasar cualquier otro valor. Este límite se aplica únicamente a los tipos de recurso de puerta de enlace de tránsito.
- `--resource-type` admite dos nuevos tipos de recursos: `TransitGateway` y `TransitGatewayAttachment`.
- `--log-format` incluye todos los campos de registro para los tipos de recursos de puerta de enlace de tránsito si no establece qué campos desea incluir. Esto solo se aplica a los tipos de recursos de puerta de enlace de tránsito.

Crear un registro de flujo

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)

Descripción de sus logs de flujo

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)

Visualización de sus registros de logs de flujo (eventos de log)

- get-log-events (AWS CLI)
- Get- CWLLog Event (AWS Tools for Windows PowerShell)

Eliminar un registro de flujo

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)

Ver los registros de flujos de AWS Transit Gateway

Consulte la información sobre los registros de flujo de su puerta de enlace de tránsito desde Amazon VPC. Cuando selecciona el recurso, se muestran todos los registros de flujo de ese recurso. La información que se muestra incluye el ID del registro de flujo, la configuración del registro de flujo y la información acerca del estado del registro de flujo.

Para ver información acerca de los registros de flujo para las puertas de enlace de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway o Transit gateway attachments (Conexión de la puerta de enlace de tránsito).
3. Seleccione una puerta de enlace de tránsito o una conexión de puerta de enlace de tránsito y elija Registros de flujo. Se mostrará información acerca de los registros de flujo en la pestaña. La columna Destination type (Tipo de destino) indica el destino en el que se publican los logs de flujo.

Gestione las etiquetas de registros de flujo de AWS Transit Gateway

Puede agregar o quitar etiquetas para un registro de flujo en las consolas de Amazon EC2 y Amazon VPC.

Para agregar o quitar etiquetas en un registro de flujo de puerta de enlace de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, elija Transit Gateway o Transit gateway attachments (Conexión de la puerta de enlace de tránsito).
3. Seleccione una puerta de enlace de tránsito o una conexión de puerta de enlace de tránsito
4. Elija Manage tags (Administrar etiquetas) para el registro de flujo requerido.
5. Para agregar una etiqueta nueva, elija Create Tag. Para quitar una etiqueta, elija el icono de eliminación (x).
6. Seleccione Save.

Buscar registros de flujos de AWS Transit Gateway

Puede buscar los registros de registro de flujo que están publicados en CloudWatch Logs mediante la consola de CloudWatch registros. Puede utilizar filtros de métricas para filtrar entradas de registro de flujo. Los registros de log de flujo están delimitados por espacios.

Para buscar registros de registro de flujo mediante la consola CloudWatch de registros

1. Abra la CloudWatch consola en https://console.aws.amazon.com/cloudwatch/.
2. En el panel de navegación, elija Registros y, luego, Grupos de registros.
3. Seleccione el grupo de registro que contiene el registro de flujo. Aparecerá una lista de flujos de registros para cada puerta de enlace de tránsito.
4. Seleccione el flujo de registro individual si conoce la puerta de enlace de tránsito que está buscando. Otra opción, elija Search Log Group (Buscar en el grupo de registro) para buscar en todo el grupo de registro. Esto puede tardar algún tiempo si hay muchas puertas de enlace de tránsito en el grupo de registro o en función del intervalo de tiempo que seleccione.
5. En Filter events (Filtrar los eventos), escriba la siguiente cadena. Esto supone que el registro de log de flujo utiliza el formato predeterminado.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport,
 protocol, packets, bytes,start,end, log_status, type,packets_lost_no_route,
 packets_lost_blackhole, packets_lost_mtu_exceeded, packets_lost_ttl_expired,
 tcp_flags,region, flow_direction, pkt_src_aws_service, pkt_dst_aws_service]
```

6. Modifique el filtro según sea necesario especificando valores para los campos. En los siguientes ejemplos se filtra por direcciones IP de origen específicas.

```
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.0.1, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
[version, resource_type, account_id,tgw_id, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr= 10.0.2.*, dstaddr,
 srcport, dstport, protocol, packets, bytes,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

El siguiente ejemplo filtra por el ID de la puerta de enlace de tránsito tgw-123abc456bca, el puerto de destino y el número de bytes.

```
[version, resource_type, account_id,tgw_id=tgw-123abc456bca, tgw_attachment_id,
 tgw_src_vpc_account_id, tgw_dst_vpc_account_id, tgw_src_vpc_id, tgw_dst_vpc_id,
 tgw_src_subnet_id, tgw_dst_subnet_id, tgw_src_eni, tgw_dst_eni, tgw_src_az_id,
 tgw_dst_az_id, tgw_pair_attachment_id, srcaddr, dstaddr, srcport, dstport =
 80 || dstport = 8080, protocol, packets, bytes >= 500,start,end, log_status,
 type,packets_lost_no_route, packets_lost_blackhole, packets_lost_mtu_exceeded,
 packets_lost_ttl_expired, tcp_flags,region, flow_direction, pkt_src_aws_service,
 pkt_dst_aws_service]
```

Eliminar un registro de registros de flujo de AWS Transit Gateway

Puede eliminar un registro de flujo de puerta de enlace de tránsito con la consola de Amazon VPC.

Estos procedimientos deshabilitan el servicio de registro de flujo para un recurso. Al eliminar un registro de flujo, no se eliminan los flujos de registro existentes de CloudWatch los registros o los archivos de registro de Amazon S3. Los datos de los registros de flujo existentes deben eliminarse con la consola del servicio correspondiente. Además, eliminar un registro de flujo que se publica en Amazon S3 no elimina las políticas de bucket ni las listas de control de acceso a los archivos de registro (ACLs).

Para eliminar un registro de flujo de puerta de enlace de tránsito

1. Abra la consola de Amazon VPC en https://console.aws.amazon.com/vpc/.
2. En el panel de navegación, seleccione Transit gateways (Puertas de enlace de tránsito).
3. Elija un ID de puerta de enlace de tránsito.
4. En la sección Registros de flujo, elija los registros de flujo que desee eliminar.
5. Elija Actions (Acciones) y, a continuación, elija Delete log group (Eliminar registros de flujo).
6. Confirme que desea eliminar el flujo seleccionando Delete (Eliminar).

Métricas y eventos en AWS Transit Gateway

Puede utilizar las siguientes características para monitorear las gateways de tránsito, analizar patrones de tráfico y solucionar problemas con las gateways de tránsito.

CloudWatch métricas

Puedes usar Amazon CloudWatch para recuperar estadísticas sobre los puntos de datos de tus pasarelas de tránsito como un conjunto ordenado de datos de series temporales, conocidos como métricas. Utilice estas métricas para comprobar que el sistema funciona de acuerdo con lo esperado. Para obtener más información, consulte CloudWatch métricas en AWS Transit Gateway.

Registros de flujo de Transit Gateway

Puede utilizar registros de flujo de las puertas de enlace de tránsito para capturar información detallada sobre el tráfico de red en las puertas de enlace de tránsito. Para obtener más información, consulte Registros de flujo de Transit Gateway.

Logs de flujo de VPC

Puede usar los registros de flujo de la VPC para capturar información detallada sobre el tráfico VPCs que entra y sale de las pasarelas de tránsito conectadas a ellas. Para obtener más información, consulte Logs de flujo de VPC en la Guía del usuario de Amazon VPC.

CloudTrail registros

Puede utilizarla AWS CloudTrail para capturar información detallada sobre las llamadas realizadas a la API de Transit Gateway y almacenarlas como archivos de registro en Amazon S3. Puede usar estos CloudTrail registros para determinar qué llamadas se realizaron, la dirección IP de origen de la llamada, quién realizó la llamada, cuándo se realizó la llamada, etc. Para obtener más información, consulte CloudTrail registra.

CloudWatch Eventos que utilizan Network Manager

Puede utilizarlos AWS Network Manager para reenviar eventos a las CloudWatch funciones o transmisiones de destino y luego enrutarlos a ellas. Network Manager genera eventos para los cambios de topología, las actualizaciones de enrutamiento y las actualizaciones de estado, todos los cuales se pueden utilizar para avisarle de los cambios en sus puertas de enlace de tránsito. Para obtener más información, consulte la guía del usuario sobre cómo monitorizar su red global con CloudWatch Events in the AWS Global Networks for Transit Gateways.

CloudWatch métricas en AWS Transit Gateway

Amazon VPC publica puntos de datos en Amazon CloudWatch para las pasarelas de tránsito y los archivos adjuntos de las pasarelas de tránsito. CloudWatchle permite recuperar estadísticas sobre esos puntos de datos como un conjunto ordenado de datos de series temporales, conocidos como métricas. Una métrica es una variable que hay que monitorizar y los puntos de datos son los valores de esa variable a lo largo del tiempo. Cada punto de datos tiene una marca temporal asociada y una unidad de medida opcional.

Puede utilizar estas métricas para comprobar si el sistema funciona de acuerdo con lo esperado. Por ejemplo, puede crear una CloudWatch alarma para supervisar una métrica específica e iniciar una acción (como enviar una notificación a una dirección de correo electrónico) si la métrica se encuentra fuera de lo que considera un rango aceptable.

Amazon VPC mide y envía sus métricas CloudWatch en intervalos de 60 segundos.

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

Contenido

Métricas de las gateways de tránsito

El espacio de nombres de `AWS/TransitGateway` incluye las siguientes métricas.

Siempre se informan todas las métricas. Sus valores dependen del tráfico que fluye por la puerta de enlace de tránsito. Consulte Dimensiones de métricas de las puertas de enlace de tránsito para conocer las dimensiones compatibles.

Métrica	Descripción
`BytesDropCountBlackhole`	El número de bytes que se perdieron por concordar con una ruta de `blackhole` . Estadísticas: la única estadística relevante es `Sum`.

Métrica	Descripción
BytesDropCountNoRoute	El número de bytes que se perdieron porque no concordaban con ninguna ruta. Estadísticas: la única estadística relevante es Sum.
BytesIn	El número de bytes recibidos por la gateway de tránsito. Estadísticas: la única estadística relevante es Sum.
BytesOut	El número de bytes enviados desde la gateway de tránsito. Estadísticas: la única estadística relevante es Sum.
PacketsIn	El número de paquetes recibidos por la gateway de tránsito. Estadísticas: la única estadística relevante es Sum.
PacketsOut	El número de paquetes enviados por la gateway de tránsito. Estadísticas: la única estadística relevante es Sum.
PacketDropCountBlackhole	El número de paquetes que se han perdido por coincidir con una ruta de blackhole . Estadísticas: la única estadística relevante es Sum.
PacketDropCountNoRoute	El número de paquetes que se han perdido porque no coincidían con ninguna ruta. Estadísticas: la única estadística relevante es Sum.
PacketDropCountTTLExpired	El número de paquetes que se han perdido porque el TTL expiró. Estadísticas: la única estadística relevante es Sum.

Métricas de nivel de conexión y zona de disponibilidad

Las siguientes métricas están disponibles para conexiones de la gateway de tránsito. Todas las métricas de conexiones se publican en la cuenta del propietario de la gateway de tránsito.

Las métricas de vinculaciones individuales también se publican en la cuenta del propietario de la vinculación. El propietario de las vinculaciones sólo puede ver las métricas de sus propias vinculaciones. Para obtener más información sobre los tipos de archivos adjuntos admitidos, consulte the section called “Vinculaciones de recursos”.

Las métricas de zona de disponibilidad están disponibles si están habilitadas para las zonas de disponibilidad (AZs) en los archivos adjuntos a las pasarelas de tránsito. Solo las conexiones de VPC admiten métricas por zona de disponibilidad. Todas las métricas de nivel de zonas de disponibilidad se publican en la cuenta del propietario de la puerta de enlace de tránsito. Las métricas de zonas de disponibilidad individuales para una vinculación también se publican en la cuenta del propietario de la vinculación. El propietario de las vinculaciones solo puede ver las métricas por zonas de disponibilidad de sus propias vinculaciones.

Siempre se informan todas las métricas. Sus valores dependen del tráfico que entra y and/or sale del adjunto a la pasarela de tránsito. Consulte Dimensiones de métricas de las puertas de enlace de tránsito para conocer las dimensiones compatibles.

Métrica	Descripción
`BytesDropCountBlackhole`	El número de bytes descartados porque concordaban con una ruta de `blackhole` en la conexión de gateway de tránsito. Estadísticas: la única estadística relevante es `Sum`.
`BytesDropCountNoRoute`	El número de bytes descartados porque no concordaban con una ruta en la conexión de la gateway de tránsito. Estadísticas: la única estadística relevante es `Sum`.
`BytesIn`	El número de bytes recibidos por la gateway de tránsito desde la conexión. Estadísticas: la única estadística relevante es `Sum`.
`BytesOut`	El número de bytes enviados desde la gateway de tránsito a la conexión. Estadísticas: la única estadística relevante es `Sum`.

Métrica	Descripción
PacketsIn	El número de paquetes recibidos por la gateway de tránsito desde la conexión. Estadísticas: la única estadística relevante es Sum.
PacketsOut	El número de paquetes enviados por la gateway de tránsito a la conexión. Estadísticas: la única estadística relevante es Sum.
PacketDropCountBlackhole	El número de paquetes descartados porque coincidían con una ruta de blackhole en la conexión de gateway de tránsito. Estadísticas: la única estadística relevante es Sum.
PacketDropCountNoRoute	El número de paquetes que se han perdido porque no coincidían con ninguna ruta. Estadísticas: la única estadística relevante es Sum.
PacketDropCountTTLExpired	El número de paquetes que se han perdido porque el TTL expiró. Estadísticas: la única estadística relevante es Sum.

Dimensiones de métricas de las puertas de enlace de tránsito

Filtra los datos de métricas de las puertas de enlace de tránsito mediante las siguientes dimensiones:

Dimensión	Descripción
TransitGateway	Filtra los datos de métrica por gateway de tránsito.
TransitGatewayAttachment	Filtra los datos de métrica por puerta de enlaces de tránsito.

Dimensión	Descripción
`TransitGateway` , `AvailabilityZone`	Filtra los datos de métricas por puerta de enlace de tránsito y por zona de disponibilidad.
`TransitGatewayAttachment` , `AvailabilityZone`	Filtra los datos de métricas por conexión de puerta de enlace de tránsito y por zona de disponibilidad.

Registre las llamadas a la API AWS Transit Gateway mediante AWS CloudTrail

AWS Transit Gateway; está integrado con AWS CloudTrailun servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un Servicio de AWS. CloudTrail captura todas las llamadas a la API de Transit Gateway como eventos. Las llamadas capturadas incluyen las llamadas desde la consola de Transit Gateway y las llamadas de código a las operaciones de la API de Transit Gateway. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó a Transit Gateway, la dirección IP desde la que se realizó la solicitud, cuándo se realizó y detalles adicionales.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales del usuario raíz o del usuario.
- Si la solicitud se realizó en nombre de un usuario de IAM Identity Center.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro Servicio de AWS.

CloudTrail está activa en tu cuenta Cuenta de AWS al crear la cuenta y automáticamente tienes acceso al historial de CloudTrail eventos. El historial de CloudTrail eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de eventos de gestión

registrados en un. Región de AWSPara obtener más información, consulte Uso del historial de CloudTrail eventos en la Guía del usuario.AWS CloudTrail La visualización del historial de eventos no conlleva ningún CloudTrail cargo.

Para tener un registro continuo de los eventos de Cuenta de AWS los últimos 90 días, crea un almacén de datos de eventos de senderos o CloudTraillagos.

CloudTrail senderos

Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. Todos los senderos creados con él Consola de administración de AWS son multirregionales. Puede crear un registro de seguimiento de una sola región o multirregionales mediante la AWS CLI. Se recomienda crear un sendero multirregional, ya que puedes capturar toda la actividad de tu Regiones de AWS cuenta. Si crea un registro de seguimiento de una sola región, solo podrá ver los eventos registrados en la Región de AWS del registro de seguimiento. Para obtener más información acerca de los registros de seguimiento, consulte Creación de un registro de seguimiento para su Cuenta de AWS y Creación de un registro de seguimiento para una organización en la Guía del usuario de AWS CloudTrail .

Puede enviar una copia de sus eventos de administración en curso a su bucket de Amazon S3 sin coste alguno CloudTrail mediante la creación de una ruta; sin embargo, hay cargos por almacenamiento en Amazon S3. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios. Para obtener información acerca de los precios de Amazon S3, consulte Precios de Amazon S3.

CloudTrail Almacenes de datos de eventos en Lake

CloudTrail Lake le permite ejecutar consultas basadas en SQL en sus eventos. CloudTrail Lake convierte los eventos existentes en formato JSON basado en filas al formato Apache ORC. ORC es un formato de almacenamiento en columnas optimizado para una recuperación rápida de datos. Los eventos se agregan en almacenes de datos de eventos, que son recopilaciones inmutables de eventos en función de criterios que se seleccionan aplicando selectores de eventos avanzados. Los selectores que se aplican a un almacén de datos de eventos controlan los eventos que perduran y están disponibles para la consulta. Para obtener más información sobre CloudTrail Lake, consulte Cómo trabajar con AWS CloudTrail Lake en la Guía del AWS CloudTrail usuario.

CloudTrail Los almacenes de datos y las consultas sobre eventos de Lake conllevan costes. Cuando crea un almacén de datos de eventos, debe elegir la opción de precios que desee utilizar para él. La opción de precios determina el costo de la incorporación y el almacenamiento de los

eventos, así como el período de retención predeterminado y máximo del almacén de datos de eventos. Para obtener más información sobre CloudTrail los precios, consulte AWS CloudTrail Precios.

Eventos de administración de Transit Gateway

Los eventos de administración proporcionan información sobre las operaciones de administración que se llevan a cabo en los recursos de su empresa Cuenta de AWS. Se denominan también operaciones del plano de control. De forma predeterminada, CloudTrail registra los eventos de administración.

AWS Transit Gateway registra todas las operaciones del plano de control de Transit Gateway como eventos de administración. Para obtener una lista de las operaciones del plano de control de AWS Transit Gateway en las que Transit Gateway inicia sesión CloudTrail, consulte las acciones de AWS Transit Gateway en la referencia de la API de Amazon EC2.

Ejemplos de eventos de Transit Gateway

Un evento representa una solicitud única de cualquier fuente e incluye información sobre la operación de API solicitada, la fecha y la hora de la operación, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que los eventos no aparecen en ningún orden específico.

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico.

Los archivos de registro incluyen los eventos de todas las llamadas a la API de tu AWS cuenta, no solo de las llamadas a la API de Transit Gateway. Puede localizar llamadas a la API de gateway de tránsito comprobando si hay elementos `eventSource` con el valor `ec2.amazonaws.com`. Para ver un registro de una acción específica (por ejemplo, `CreateTransitGateway`), compruebe la existencia de elementos `eventName` con el nombre de la acción.

A continuación, se muestra un ejemplo de CloudTrail registro de la API de Transit Gateway para un usuario que creó una pasarela de tránsito mediante la consola. Puede identificar la consola mediante

el elemento `userAgent`. Puede identificar la llamada a la API solicitada mediante los elementos `eventName`. Encontrará la información sobre el usuario (`Alice`) en el elemento `userIdentity`.

Example Ejemplo: CreateTransitGateway


```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "Alice"
    },
    "eventTime": "2018-11-15T05:25:50Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "CreateTransitGateway",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.ec2.amazonaws.com",
    "requestParameters": {
        "CreateTransitGatewayRequest": {
            "Options": {
                "DefaultRouteTablePropagation": "enable",
                "AutoAcceptSharedAttachments": "disable",
                "DefaultRouteTableAssociation": "enable",
                "VpnEcmpSupport": "enable",
                "DnsSupport": "enable"
            },
            "TagSpecification": {
                "ResourceType": "transit-gateway",
                "tag": 1,
                "Tag": {
                    "Value": "my-tgw",
                    "tag": 1,
                    "Key": "Name"
                }
            }
        }
    },
    "responseElements": {
        "CreateTransitGatewayResponse": {
            "xmlns": "http://ec2.amazonaws.com/doc/2016-11-15/",
```

```
            "requestId": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
            "transitGateway": {
                "tagSet": {
                    "item": {
                        "value": "my-tgw",
                        "key": "Name"
                    }
                },
                "creationTime": "2018-11-15T05:25:50.000Z",
                "transitGatewayId": "tgw-0a13743bd6c1f5fcb",
                "options": {
                    "propagationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a",
                    "amazonSideAsn": 64512,
                    "defaultRouteTablePropagation": "enable",
                    "vpnEcmpSupport": "enable",
                    "autoAcceptSharedAttachments": "disable",
                    "defaultRouteTableAssociation": "enable",
                    "dnsSupport": "enable",
                    "associationDefaultRouteTableId": "tgw-rtb-0123cd602be10b00a"
                },
                "state": "pending",
                "ownerId": 123456789012
            }
        }
    },
    "requestID": "a07c1edf-c201-4e44-bffb-3ce90EXAMPLE",
    "eventID": "e8fa575f-4964-4ab9-8ca4-6b5b4EXAMPLE",
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Gestión de identidad y acceso en AWS Transit Gateway

AWS utiliza credenciales de seguridad para identificarlo y concederle acceso a sus AWS recursos. Puede utilizar las funciones de AWS Identity and Access Management (IAM) para permitir que otros usuarios, servicios y aplicaciones utilicen sus AWS recursos de forma completa o limitada, sin compartir sus credenciales de seguridad.

De forma predeterminada, los usuarios de IAM no tienen permiso para crear, ver o modificar AWS recursos. Para permitir que un usuario acceda a los recursos, por ejemplo, una puerta de enlace de tránsito y realice tareas, debe crear una política de IAM que conceda al usuario permiso para utilizar los recursos específicos y las acciones de API que necesita. A continuación, asocie la política al usuario al grupo al que pertenece el usuario. Cuando se asocia una política a un usuario o grupo de usuarios, les otorga o deniega el permiso para realizar las tareas especificadas en los recursos indicados.

Para trabajar con una pasarela de tránsito, una de las siguientes políticas AWS gestionadas podría satisfacer tus necesidades:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

Políticas de ejemplo para administrar las puerta de enlaces de tránsito

A continuación, se muestran políticas de IAM de ejemplo para el trabajo con puerta de enlaces de tránsito.

Crear una puerta de enlace de tránsito con las etiquetas obligatorias

El siguiente ejemplo permite a los usuarios crear una puerta de enlace de tránsito. La clave de condición `aws:RequestTag` precisa que los usuarios etiqueten la puerta de enlace de tránsito con la etiqueta `stack=prod`. La clave de condición `aws:TagKeys` utiliza el modificador `ForAllValues` para indicar que solo la clave `stack` está permitida en la solicitud (no se puede especificar ninguna

otra etiqueta). Si los usuarios no transmiten esta etiqueta en concreto cuando crean la puerta de enlace de tránsito o si no especifican ninguna etiqueta, la solicitud dará un error.

La segunda instrucción utiliza la clave de condición `ec2:CreateAction` para permitir a los usuarios crear etiquetas únicamente en el contexto de `CreateTransitGateway`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateTransitGateway"
                }
            }
        }
    ]
}
```

Usar tablas de enrutamiento de puerta de enlaces de tránsito

El siguiente ejemplo permite a los usuarios crear y eliminar tablas de ruteo de puerta de enlace de tránsito solo para una puerta de enlace de tránsito específica (`tgw-11223344556677889`). Los usuarios también crean y sustituyen rutas en cualquier tabla de enrutamiento de puerta de enlace de tránsito, pero solo para las vinculaciones que tienen la etiqueta `network=new-york-office`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1:123456789012:transit-gateway/
tgw-11223344556677889",
                "arn:aws:ec2:*:*:transit-gateway-route-table/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-attachment/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/network": "new-york-office"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTransitGatewayRoute",
                "ec2:ReplaceTransitGatewayRoute"
```

```
            ],
            "Resource": "arn:aws:ec2:*:*:transit-gateway-route-table/*"
        }
    ]
}
```

Utilice funciones vinculadas al servicio para las pasarelas de tránsito en AWS Transit Gateway

Amazon VPC utiliza roles vinculados a servicios para los permisos que necesita para llamar a otros servicios de AWS en su nombre. Para obtener más información, consulte Service-linkedlos roles en la Guía del usuario de IAM.

Rol vinculado a servicios de la puerta de enlace de tránsito

Amazon VPC utiliza roles vinculados a servicios para los permisos que necesita para llamar a otros servicios AWS en su nombre cuando trabaja con una puerta de enlace de tránsito.

Permisos concedidos por el rol vinculado a servicios

Amazon VPC utiliza el rol vinculado al servicio denominado AWSServiceRoleForVPCTransitGatewaypara realizar las siguientes acciones en su nombre cuando trabaja con una pasarela de tránsito:

- `ec2:CreateNetworkInterface`
- `ec2:DescribeNetworkInterfaces`
- `ec2:ModifyNetworkInterfaceAttribute`
- `ec2:DeleteNetworkInterface`
- `ec2:CreateNetworkInterfacePermission`
- `ec2:AssignIpv6Addresses`
- `ec2:UnAssignIpv6Addresses`

El AWSServiceRoleForVPCTransitGatewayrol confía en los siguientes servicios para asumir el rol:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGatewayutiliza la política gestionadaAWSVPCTransitGatewayServiceRolePolicy.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte los permisos de Service-linked rol en la Guía del usuario de IAM.

Creación del rol vinculado a servicios

No necesita crear manualmente un rol AWSServiceRoleForVPCTransitGateway. Amazon VPC crea este rol para cuando se asocia una VPC de la cuenta a una puerta de enlace de tránsito.

Editar el rol vinculado a servicios

Puede utilizar IAM para editar la descripción de AWSServiceRoleForVPCTransitGateway. Para obtener más información, consulte la Descripción sobre cómo editar un rol vinculado al servicio en la Guía del usuario de IAM.

Eliminar el rol vinculado a servicios

Si ya no necesita usar las pasarelas de tránsito, le recomendamos que las elimine. AWSServiceRoleForVPCTransitGateway

Puedes eliminar este rol vinculado al servicio solo después de eliminar todos los adjuntos de VPC de Transit Gateway de tu cuenta. AWS Esto garantiza que no pueda eliminar accidentalmente el permiso para acceder a sus vinculaciones de VPC.

Puede utilizar la consola, la CLI o la API de IAM para eliminar los roles vinculados a servicios. Para obtener más información, consulte Eliminación de un rol vinculado a servicios en la Guía del usuario de IAM.

Tras la eliminación AWSServiceRoleForVPCTransitGateway, Amazon VPC vuelve a crear el rol si adjuntas una VPC de tu cuenta a una pasarela de tránsito.

AWS gestionó las políticas para las pasarelas de tránsito en AWS Transit Gateway

Una política AWS gestionada es una política independiente creada y administrada por. AWS AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

Para trabajar con una pasarela de tránsito, una de las siguientes políticas AWS gestionadas podría satisfacer tus necesidades:

- AmazonEC2FullAccess
- AmazonEC2ReadOnlyAccess
- PowerUserAccess
- ReadOnlyAccess

AWS política gestionada: AWSVPCTransitGatewayServiceRolePolicy

Esta política está asociada a la función AWSServiceRoleForVPCTransitGateway. Esto permite a Amazon VPC crear y administrar recursos para las conexiones de puerta de enlace de tránsito.

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

Transit Gateway se actualiza a AWS políticas administradas

Consulte los detalles sobre las actualizaciones de las políticas AWS gestionadas para las pasarelas de tránsito desde que Amazon VPC comenzó a realizar el seguimiento de estos cambios en marzo de 2021.

Cambio	Descripción	Fecha
Amazon VPC comenzó a hacer un seguimiento de los cambios	Amazon VPC comenzó a realizar un seguimiento de los cambios en sus políticas AWS gestionadas.	1 de marzo de 2021

ACL de red para pasarelas de tránsito en AWS Transit Gateway

Una lista de control de acceso a la red (NACL) es una capa opcional de seguridad.

Las reglas de la lista de control de acceso a la red (NACL) se aplican de manera diferente, en función del escenario:

- the section called “Misma subred para instancias EC2 y la asociación de puerta de enlace de tránsito”
- the section called “Diferentes subredes para instancias EC2 y la asociación de puerta de enlace de tránsito”

Misma subred para instancias EC2 y la asociación de puerta de enlace de tránsito

Considere una configuración en la que tenga instancias de EC2 y una asociación de puerta de enlace de tránsito en la misma subred. La misma ACL de red se utiliza para el tráfico de las instancias EC2 a la puerta de enlace de tránsito y para el tráfico proveniente de la puerta de enlace de tránsito a las instancias.

Las reglas de NACL se aplican de la siguiente manera para el tráfico de instancias para la puerta de enlace de tránsito:

- Las reglas de salida utilizan la dirección IP de destino para la evaluación.
- Las reglas de entrada utilizan la dirección IP de origen para la evaluación.

Las reglas de NACL se aplican de la siguiente manera para el tráfico proveniente de la puerta de enlace de tránsito hacia las instancias:

- Las reglas de salida no se evalúan.
- Las reglas de entrada no se evalúan.

Diferentes subredes para instancias EC2 y la asociación de puerta de enlace de tránsito

Considere una configuración en la que tenga instancias EC2 en una subred y una asociación de puerta de enlace de tránsito en una subred diferente, y cada subred está asociada a una ACL de red diferente.

Las reglas de una ACL de red se aplican de la siguiente manera para la subred de instancias EC2:

- Las reglas de salida utilizan la dirección IP de destino para evaluar el tráfico de las instancias a la puerta de enlace de tránsito.
- Las reglas de salida utilizan la dirección IP de destino para evaluar el tráfico de la puerta de enlace de tránsito a las instancias.

Las reglas NACL se aplican de la siguiente manera para la subred de la puerta de enlace de tránsito:

- Las reglas de salida utilizan la dirección IP de destino para evaluar el tráfico de la puerta de enlace de tránsito a las instancias.
- Las reglas de salida no se utilizan para evaluar el tráfico de las instancias a la puerta de enlace de tránsito.
- Las reglas de entrada utilizan la dirección IP de origen para evaluar el tráfico de las instancias a la puerta de enlace de tránsito.
- Las reglas de entrada no se utilizan para evaluar el tráfico de la puerta de enlace de tránsito a las instancias.

Prácticas recomendadas

Utilice una subred independiente para cada archivo asociado a la VPC de la puerta de enlace de tránsito. En cada subred, utilice un CIDR pequeño, por ejemplo /28, a fin de tener más direcciones para los recursos de EC2. Cuando utilice una subred independiente, puede configurar los siguientes recursos:

- Mantenga abierta la NACL entrante y saliente asociada con las subredes de la puerta de enlace de tránsito.
- En función del flujo de tráfico, puede aplicar NACL a las subredes de carga de trabajo.

Para obtener más información sobre cómo funcionan las conexiones de VPC, consulte the section called “Vinculaciones de recursos”.

AWS Cuotas de Transit Gateway

Cuenta de AWS Tiene las siguientes cuotas (anteriormente denominadas límites) en relación con las pasarelas de tránsito. A menos que se indique lo contrario, cada cuota es específica de la región.

La consola de Service Quotas proporciona información sobre las cuotas de su cuenta. Puede utilizar la consola de Service Quotas para consultar las cuotas predeterminadas y solicitar aumentos de cuota para las cuotas ajustables. Para obtener más información, consulte este tema acerca de cómo solicitar un aumento de cuota en la Guía del usuario de Service Quotas.

Si todavía no hay disponible una cuota ajustable en Service Quotas, puede abrir un caso de soporte.

General

Name	Predeterminado	Ajustable
Puertas de enlace de tránsito por cuenta	5	Sí
Bloques de CIDR por puerta de enlace de tránsito	5	No

Los bloques de CIDR se utilizan en la característica the section called “Conexiones y pares de Connect”.

Enrutamiento

Name	Predeterminado	Ajustable
Tablas de enrutamiento de puerta de enlace de tránsito por puerta de enlace de tránsito	20	Sí
Total de rutas combinadas (dinámicas y estáticas) en todas las tablas de rutas para una única puerta de enlace de tránsito	10 000	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico

Name	Predeterminado	Ajustable
		de cuentas (TAM) para obtener más ayuda.
Rutas dinámicas anunciadas desde un dispositivo de enrutador virtual a una interconexión de Connect	1 000	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Rutas anunciadas desde una interconexión de Connect en una puerta de enlace de tránsito hasta un dispositivo de enrutador virtual	5 000	No
Número de rutas estáticas para un prefijo hacia una sola conexión	1	No

Las rutas anunciadas proceden de la tabla de enrutamiento vinculada a la conexión de Connect.

Vinculaciones de las puerta de enlaces de tránsito

Una puerta de enlace de tránsito no puede tener más de una vinculación para la misma VPC.

Name	Predeterminado	Ajustable
Conexiones por puerta de enlace de tránsito	5 000	Sí
Gateways de tránsito por VPC	5	No
Vinculaciones de interconexiones por puerta de enlace de tránsito	50	Sí
Vinculaciones de interconexiones pendientes por puerta de enlace de tránsito	10	Sí

Name	Predeterminado	Ajustable
Vinculaciones de interconexiones entre dos puertas de enlace de tránsito o entre una puerta de enlace de tránsito y una periferia de red central (CNE) de Cloud WAN	1	No
Interconexiones de Connect (túneles GRE) por vinculación de Connect	4	No
Concentradores de VPN por pasarela de tránsito	5	No
Conexiones VPN por concentrador VPN	100	No

Ancho de banda

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. Para los adjuntos de VPC, las puertas de enlace de Direct Connect o en las conexiones de puerta de enlace de tránsito interconectadas, intentaremos proporcionar un ancho de banda adicional que supere el valor predeterminado.

Name	Predeterminado	Ajustable
Ancho de banda por adjunto de VPC por zona de disponibilidad	Hasta 100 Gbps en cada dirección (es decir, 100 Gbps de entrada y 100 Gbps de salida)	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Paquetes por segundo por cada puerta de enlace de tránsito (adjunto de VPC) y por zona de disponibilidad	Hasta 7 500 000	Póngase en contacto con su arquitecto de soluciones (SA) o su

Name	Predeterminado	Ajustable
		administrador técnico de cuentas (TAM) para obtener más ayuda.
Ancho de banda para la conexión de Direct Connect pasarela o pasarela de tránsito interconectada por zona de disponibilidad disponible en la región	Hasta 100 Gbps en cada dirección (es decir, 100 Gbps de entrada y 100 Gbps de salida)	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Paquetes por segundo por adjunto a la pasarela de tránsito (Direct Connect y adjuntos de interconexión) por zona de disponibilidad disponible en la región	Hasta 7 500 000	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Ancho de banda máximo por interconexión de Connect (túnel de GRE) por conexión de Connect	Hasta 5 Gbps	No
Cantidad máxima de paquetes por segundo y por par de Connect	Hasta 300 000	No

Puede utilizar el enrutamiento de varias rutas de igual costo (ECMP) para obtener un ancho de banda de VPN superior mediante la incorporación de varios túneles de VPN. Para utilizar ECMP, la conexión de VPN debe estar configurada para el enrutamiento dinámico. ECMP no es compatible con conexiones de VPN que utilizan enrutamiento estático.

Puede crear hasta 4 pares de Connect por adjunto de Connect (hasta 20 Gbps de ancho de banda total por adjunto de Connect), siempre que el adjunto de transporte subyacente (VPC Direct Connect o) soporte el ancho de banda requerido. Puede utilizar el ECMP para obtener un mayor ancho

de banda al escalar horizontalmente a través de varios interconexiones de Connect de la misma conexión de Connect o a través de varias conexiones de Connect en la misma puerta de enlace de tránsito. La gateway de tránsito no puede utilizar ECMP entre los pares de BGP del mismo par de Connect.

Para conocer los límites de ancho de banda y paquetes con un túnel VPN, consulte el ancho de banda y el rendimiento de la VPN.

Direct Connect pasarelas

Name	Predeterminado	Ajustable
Direct Connect pasarelas por pasarela de tránsito	20	No
Pasarelas de tránsito por pasarela Direct Connect	6	No

Unidad de transmisión máxima (MTU).

- La unidad de transmisión máxima (MTU) de una conexión de red es el tamaño, en bytes, del mayor paquete permitido que se puede transferir a través de la conexión. Cuanto mayor sea la MTU de una conexión, mayor cantidad de datos se podrán transferir en un solo paquete. Una puerta de enlace de tránsito admite una MTU de 8500 bytes para el tráfico entre VPCs Transit Gateway Connect y los adjuntos de emparejamiento (adjuntos de emparejamiento intrarregionales, interregionales y de WAN en la nube). Direct Connect El tráfico a través de conexiones de VPN puede tener una MTU de 1500 bytes.
- Al migrar desde el emparejamiento de VPC para utilizar una puerta de enlace de tránsito, una discrepancia en el tamaño de la MTU entre el emparejamiento de VPC y la puerta de enlace de tránsito podría provocar la caída de algunos paquetes de tráfico asimétricos. Actualice ambas VPCs al mismo tiempo para evitar que los paquetes gigantes se caigan debido a una falta de coincidencia de tamaño.
- La puerta de enlace de tránsito aplica el bloqueo de tamaño máximo del segmento (MSS) a todos los paquetes. Para obtener más información, consulte RFC879.
- Para obtener más información sobre las cuotas de Site-to-Site VPN para MTU, consulte Unidad máxima de transmisión (MTU) en la Guía del usuario.AWS Site-to-Site VPN

- Las puertas de enlace de tránsito admiten Path MTU Discovery (PMTUD) para el tráfico que ingresa a las conexiones de VPC y Connect. La puerta de enlace de tránsito genera los ICMPv4 paquetes `FRAG_NEEDED` para y `Packet Too Big (PTB)` para ICMPv6 los paquetes. Las pasarelas de tránsito no admiten PMTUD en los archivos adjuntos de Site-to-site VPN, Direct Connect y Peering. Para obtener más información sobre Path MTU Discovery, consulte Path MTU Discovery en la Guía del usuario de Amazon VPC.

Multidifusión

> **Note**
>
> Es posible que la multidifusión de la puerta de enlace de tránsito no sea adecuada para operaciones de alta frecuencia o aplicaciones sensibles al rendimiento. Le aconsejamos encarecidamente que revise primero los siguientes límites de multidifusión. Póngase en contacto con el equipo de su cuenta o de arquitectos de soluciones para obtener una revisión detallada de sus requisitos de rendimiento.

Name	Predeterminado	Ajustable
Dominios de multidifusión por puerta de enlace de tránsito	20	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Interfaces de red de multidifusión por puerta de enlace de tránsito	10 000	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.

Name	Predeterminado	Ajustable
Asociaciones de dominios de multidifusión por VPC	20	Póngase en contacto con su arquitecto de soluciones (SA) o su administrador técnico de cuentas (TAM) para obtener más ayuda.
Miembros y fuentes de grupos estáticos y de IGMPv2 multidifusión por pasarela de tránsito	10 000	No
Miembros de grupos estáticos y de IGMPv2 multidifusión por grupo de multidifusión de la puerta de enlace de tránsito	100	No
Rendimiento máximo de multidifusión por flujo	1 Gbps	No
Rendimiento máximo de multidifusión agregado por zona de disponibilidad	20 Gbps	No
Paquetes máximos por segundo por flujo (menos de 10 receptores)	75 000	No
Paquetes máximos por segundo por flujo (más de 10 receptores)	15.000	No
Cantidad máxima de paquetes agregados por segundo (menos de 10 receptores)	2 500 000	No
Cantidad máxima de paquetes agregados por segundo (más de 10 receptores)	500.000	No

AWS Administrador de redes

Nombre	Predeterminado	Ajustable
Redes globales por Cuenta de AWS	5	Sí
Dispositivos por red global	200	Sí
Enlaces por red global	200	Sí
Sitios por red global	200	Sí
Conexiones por red global	500	No

Recursos de cuotas adicionales

Para obtener más información, consulte los siguientes temas:

- Site-to-Site Cuotas de VPN en la Guía AWS Site-to-Site VPN del usuario
- Cuotas de Amazon VPC en la Guía del usuario de Amazon VPC
- Cuotas de Direct Connect en la Guía del usuario de AWS Direct Connect

Historial de documentos para puerta de enlaces de tránsito

En la tabla siguiente se describen las versiones de las puerta de enlaces de tránsito.

Cambio	Descripción	Fecha
Archivos adjuntos de Client VPN	Cree un adjunto de Client VPN para conectar una pasarela de tránsito a un punto final de Client VPN.	20 de abril de 2026
Asignación flexible de costos	Configure políticas flexibles de asignación de costos para controlar cómo se distribuyen los costos de procesamiento y transferencia de datos en toda su organización.	20 de noviembre de 2025
Encryption Support para pasarelas de tránsito	Administrar el soporte de cifrado en las pasarelas de tránsito para aplicar el cifrado en tránsito a todo el tráfico.	20 de noviembre de 2025
Vinculaciones de funciones de red	Cree una conexión de función de red a la cual conectar de manera directa una puerta de enlace de tránsito de AWS Network Firewall.	16 de junio de 2025
Compatibilidad de referencia a grupos de seguridad	Ahora puede hacer referenci a a un grupo de seguridad en las VPC conectadas a una puerta de enlace de tránsito.	25 de septiembre de 2024
AWS Cuotas de Transit Gateway	Se agregaron límites de ancho de banda.	14 de agosto de 2023

AWS Registros de flujo de Transit Gateway	Las puertas de enlace de tránsito ahora admiten registros de flujo de Transit Gateway, lo que le permite monitorear y registrar el tráfico de red entre las puertas de enlace.	14 de julio de 2022
Tablas de políticas de la puerta de enlace de tránsito	Utilice tablas de políticas para configurar el enrutamiento dinámico de las puertas de enlace de tránsito para el intercambio automático de información de enrutamiento y accesibilidad con tipos de puertas de enlace de tránsito interconectadas.	13 de julio de 2022
Guía del usuario de Network Manager	Network Manager se creó como guía independiente y ya no se incluye como parte de la Guía del usuario de AWS Transit Gateway.	2 de diciembre de 2021
Vinculaciones de interconexiones	Puede crear una interconexión con una puerta de enlace de tránsito en la misma región.	1 de diciembre de 2021
Transit Gateway Connect	Puede establecer una conexión entre una puerta de enlace de tránsito y dispositivos virtuales de terceros que se ejecutan en una VPC.	10 de diciembre de 2020

Modo Dispositivo	Puede habilitar el modo dispositivo en una conexión de la VPC para garantizar que el tráfico bidireccional fluya a través de la misma zona de disponibilidad para la conexión.	29 de octubre de 2020
Referencias de lista de prefijos	Puede hacer referencia a una lista de prefijos en la tabla de enrutamiento de la puerta de enlace de tránsito.	24 de agosto de 2020
Modificar puerta de enlace de tránsito	Puede modificar las opciones de configuración de la puerta de enlace de tránsito.	24 de agosto de 2020
CloudWatch métricas para los archivos adjuntos de Transit Gateway	Puede ver CloudWatch las métricas de los archivos adjuntos de las pasarelas de tránsito individuales.	6 de julio de 2020
Analizador de rutas de Administrador de red	Puede analizar las rutas en las tablas de enrutamiento de la puerta de enlace de tránsito en su red global.	4 de mayo de 2020
Vinculaciones de interconexiones	Puede crear una interconexión con una puerta de enlace de tránsito en otra región.	3 de diciembre de 2019

Soporte multidifusión	La puerta de enlace de tránsito es compatible con el tráfico multidifusión de direccionamiento entre las subredes de VPC asociados y funciona como un enrutador multidifusión para las instancias que envían tráfico destinado a varias instancias de recepción.	3 de diciembre de 2019
AWS Administrador de red	Puede visualizar y supervisar sus redes globales que estén construidas alrededor de las puerta de enlaces de tránsito.	3 de diciembre de 2019
AWS Direct Connect soporte	Puede usar una Direct Connect puerta de enlace para conectar su Direct Connect conexión a través de una interfaz virtual de tránsito a las VPC o VPN conectadas a su puerta de enlace de tránsito.	27 de marzo de 2019
Versión inicial	Esta versión presenta puerta de enlaces de tránsito.	26 de noviembre de 2018

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.