AWS Transit Gateway

Amazon VPC

Amazon VPC: AWS Transit Gateway

Table of Contents

¿Qué es Amazon VPC Transit Gateways?

Amazon VPC Transit Gateways es un centro de tránsito de red que se utiliza para interconectar nubes privadas virtuales (VPCs) 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 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 más VPCs
  - Un dispositivo de red de terceros/SD-WAN de 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
  - Un accesorio de función de red. Para obtener más información, consulte the section called "Adjuntos 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 VPCs Transit Gateway Connect y los adjuntos de emparejamiento (adjuntos de emparejamiento intrarregionales, interregionales y de WAN en la nube). AWS Direct Connect El tráfico a través de conexiones de VPN puede tener una MTU de 1500 bytes.
- 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:

- AWS Management Console — 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 SDKs— 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 SDKs.

- 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, consulta la referencia de la EC2 API de Amazon.

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. Para obtener más información, consulte Precios de AWS Transit Gateway.

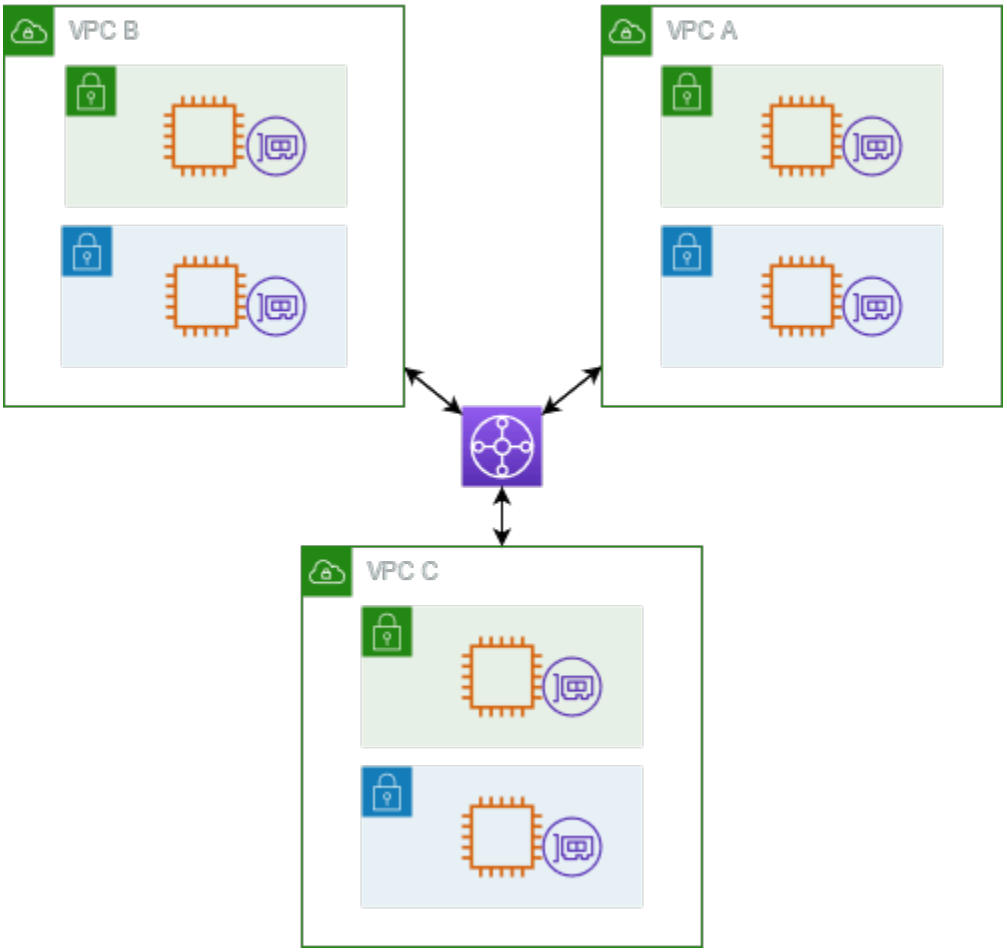
Cómo funciona Amazon VPC Transit Gateways

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 (VPCs) 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 rutas de cada una de ellas VPCs incluye la ruta local y las rutas que envían el tráfico destinado a las otras dos VPCs a la pasarela 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 VPCs. 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
- Una o más puertas de enlace AWS Direct Connect
- 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 vincular una VPC con un CIDR 10.1.0.0/16 a una segunda VPC que utilice el mismo CIDR a una puerta de enlace de tránsito, y a continuación, configurar 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 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.

> **Note**
>
> - No se admite BGP Multipath AS-Path Relax, por lo que no se puede utilizar el ECMP en distintos números de sistemas autónomos (). ASNs
> - 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, el tráfico se puede dirigir a todas las subredes en la VPC, no solo a la subred especificada o la zona de disponibilidad. 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

Su puerta de enlace de tránsito enruta IPv4 y IPv6 empaqueta entre los archivos adjuntos mediante las tablas de rutas de Transit Gateway. Puede configurar estas tablas de enrutamiento para propagar las rutas desde las tablas de enrutamiento para las conexiones VPN conectadas VPCs y las puertas de enlace 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 se crea una tabla de rutas predeterminada para la puerta de enlace 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 una conexión de VPN o una vinculación de puerta de enlace de Direct Connect, puede propagar las rutas aprendidas desde el enrutador en las instalaciones mediante BGP a cualquiera de las tablas de enrutamiento de Transit Gateway.

Cuando se utiliza el enrutamiento dinámico con una conexión de VPN, las rutas de la tabla de enrutamiento asociadas con la conexión de VPN se anuncian en la puerta de enlace de cliente a través de BGP.

Para una conexión de Connect, las rutas de la tabla de enrutamiento asociada a la conexión de Connect se anuncian a los dispositivos virtuales de terceros, como dispositivos SD-WAN, 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
  - Rutas propagadas por la VPC
  - Rutas propagadas por la puerta de enlace de Direct Connect
  - Rutas propagadas por Transit Gateway Connect
  - Site-to-Site VPN a través de rutas privadas propagadas por Direct Connect
  - Site-to-Site Rutas propagadas por 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 pasarela de tránsito sin MED, AWS Transit Gateway asignará los siguientes valores predeterminados:
>   - 0 para las rutas entrantes anunciadas en los archivos adjuntos de Direct Connect.
>   - 100 para las rutas entrantes anunciadas en los archivos adjuntos de VPN y 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	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 AWS 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	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
172.31.0.0/16	tgw-attach-456 | dxgw_id	AWS Direct Connect gateway	Propagado	3
172.31.0.0/16	tgw-attach-789 | -123 tgw-connect-peer	Conectar	Propagado	4
172.31.0.0/16	tgw-attach-789 | vpn-5678	VPN	Propagado	5

Adjuntos 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 la pasarela de transporte. Elimina la necesidad de crear y gestionar la inspección manualmente VPCs.

Con un accesorio de función de red:

- AWS crea y administra automáticamente la infraestructura subyacente
- El tráfico se puede inspeccionar a medida que pasa por su pasarela de transporte
- Las políticas de seguridad se aplican de forma coherente en toda la red

- Puede dirigir el tráfico a través del firewall mediante reglas de enrutamiento sencillas
- El adjunto funciona en varias zonas de disponibilidad para lograr 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 finales separados por separado. VPCs

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 un adjunto de Network Firewall con el modo dispositivo activado automáticamente. Esto elimina la necesidad de gestionar la inspección de forma explícita VPCs.

Con la integración de Network Firewall, ya no necesita crear y gestionar la inspección VPCs de sus despliegues de Network Firewall. En lugar de seleccionar una VPC y subredes al crear el firewall, selecciona directamente el Transit Gateway y aprovisiona y administra AWS automáticamente todos los recursos necesarios entre bastidores. Verás un nuevo accesorio de función de red de Transit Gateway en lugar de un punto final de firewall individual.

En situaciones con varias cuentas, la memoria RAM de Transit Gateway se puede compartir entre el propietario de Transit Gateway y la cuenta propietaria del Network Firewall, lo que permite a cualquiera de las cuentas gestionar el adjunto del firewall. Una vez que el firewall y el archivo adjunto estén listos, solo tiene que modificar las tablas de rutas de Transit Gateway para enviar el tráfico al archivo adjunto para su inspección.

> **Note**
>
> - Transit Gateway solo admite el enrutamiento estático en los archivos adjuntos de Network Firewall.
> - No se admiten firewalls de terceros.

Para obtener más información sobre los firewalls y los archivos adjuntos, consulte los archivos adjuntos a las funciones de red de Transit Gateway.

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.

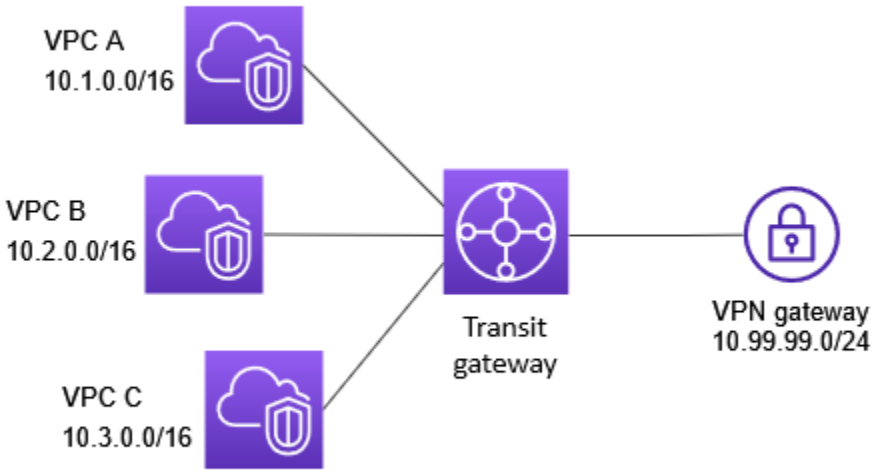
Ejemplo: enrutador centralizado

Puedes configurar tu pasarela de tránsito como un router centralizado que conecte todas tus VPCs conexiones y las de 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

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 VPCs. 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 pasarela 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 la VPC CIDRs se agrega a la tabla de 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 entrada es la entrada predeterminada para el IPv4 enrutamiento local en la VPC; esta entrada permite que las instancias de esta VPC se comuniquen entre sí. La segunda entrada enruta el resto del tráfico de IPv4 subred a la puerta de enlace de tránsito. La siguiente table muestra las rutas de VPC A.

Destino	Objetivo
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 BGP de la puerta de enlace del cliente contiene la siguiente VPC CIDRs.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

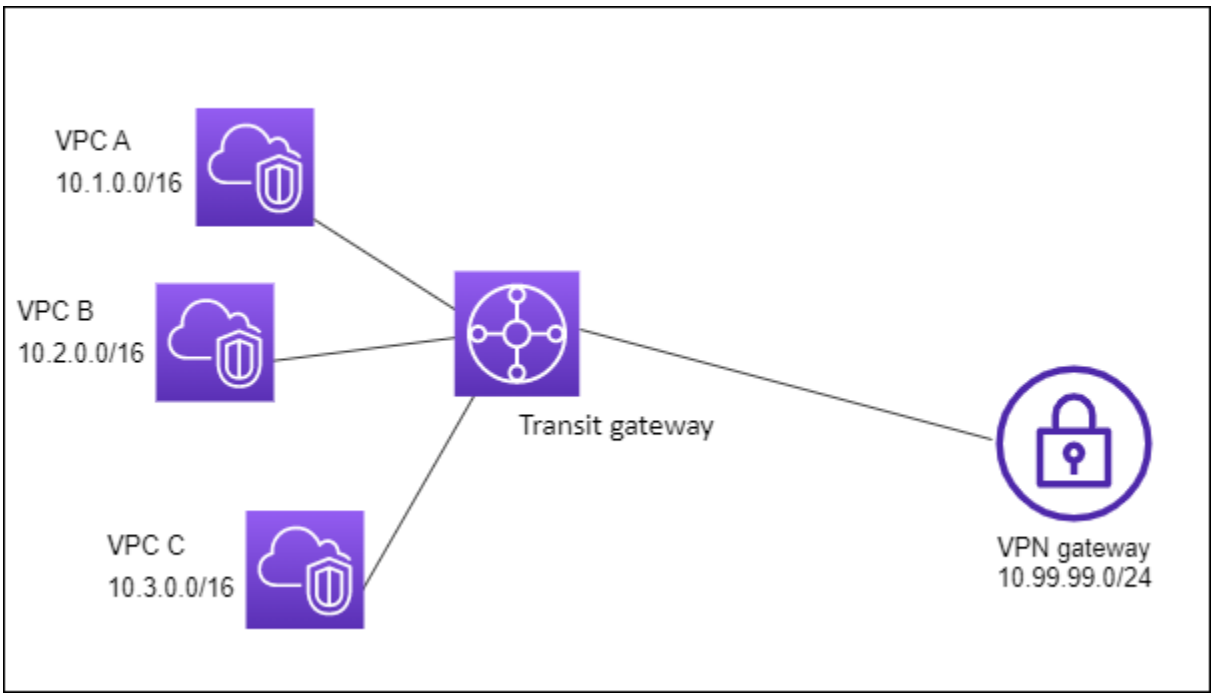
Ejemplo: aislado VPCs

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

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 VPCs. 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 accesorios en la puerta de tránsito para los tres VPCs. Para obtener más información, consulte the section called “Crear una conexión de VPC”.
- Un adjunto de Site-to-Site VPN en la pasarela 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 VPN está activa, se establece la sesión de BGP y el CIDR de la VPN se propaga a la tabla de rutas de la puerta de enlace de tránsito y la VPC CIDRs se agrega a la tabla de BGP de la puerta de enlace del cliente.

Enrutamiento

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

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

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

Destino	Objetivo
10.1.0.0/16	local
0.0.0.0/0	tgw-id

Tablas de enrutamiento de la puerta de enlace de tránsito

En este escenario, se utiliza una tabla de rutas para la conexión VPN VPCs y otra tabla de rutas para la conexión 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

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 Habilitación de la propagación de rutas en la tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways.

Tabla del BGP de la puerta de enlace de cliente

La tabla BGP de la puerta de enlace del cliente contiene la siguiente VPC CIDRs.

- 10.1.0.0/16
- 10.2.0.0/16
- 10.3.0.0/16

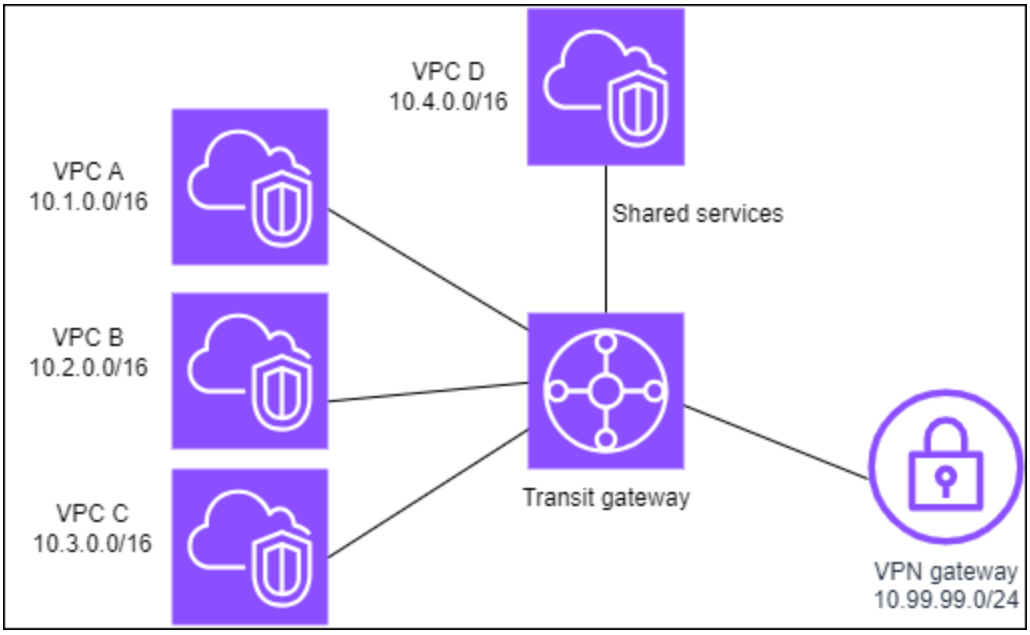
Ejemplo: aislada VPCs con servicios compartidos

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

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 se enrutan primero 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. VPCs 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 pasarela 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 VPN está activa, se establece la sesión de BGP y el CIDR de la VPN se propaga a la tabla de rutas de la puerta de enlace de tránsito y la VPC CIDRs se agrega a la tabla de BGP de la puerta de enlace del 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 la VPC de conexión VPN VPCs y servicios compartidos y otra para ella.

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 IPv4 subred a la puerta de enlace de tránsito.

Destino	Objetivo
10.1.0.0/16	local
0.0.0.0/0	*transit gateway ID*

Tablas de enrutamiento de la puerta de enlace de tránsito

En este escenario, se utiliza una tabla de rutas para la conexión VPN VPCs y otra tabla de rutas para la conexión 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 VPCs 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 Habilitación de la propagación de rutas en la tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways.

Tabla del BGP de la puerta de enlace de cliente

La tabla BGP de la puerta de enlace del cliente contiene CIDRs los cuatro. VPCs

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.

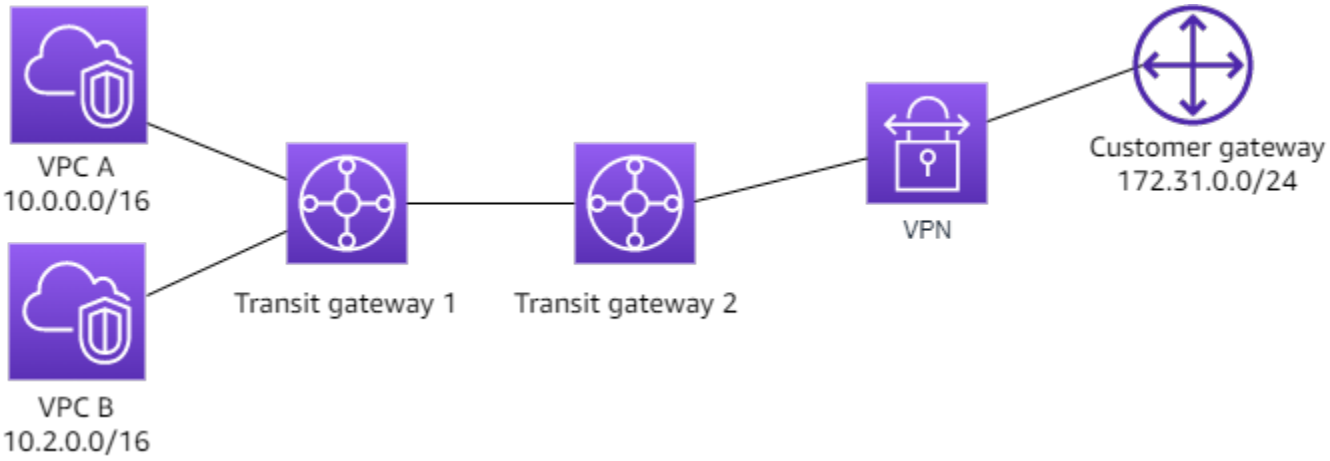
Contenido

- Descripción general

- Recursos
- Enrutamiento

Descripción general

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 VPCs. 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 pasarela 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 Amazon VPC Transit Gateways.

Al crear los adjuntos de la VPC, los de cada VPC se propagan a la CIDRs tabla de enrutamiento de la puerta de enlace 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 puerta de enlace de tránsito 2
- Las VPC CIDRs se agregan a la tabla BGP de la puerta de enlace del 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 entrada es la entrada predeterminada para el IPv4 enrutamiento local en 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 IPv4 subred a la puerta de enlace de tránsito. La siguiente table muestra las rutas de VPC A.

Destino	Objetivo
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
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 BGP de la puerta de enlace del cliente contiene la siguiente VPC CIDRs.

- 10.0.0.0/16
- 10.2.0.0/16

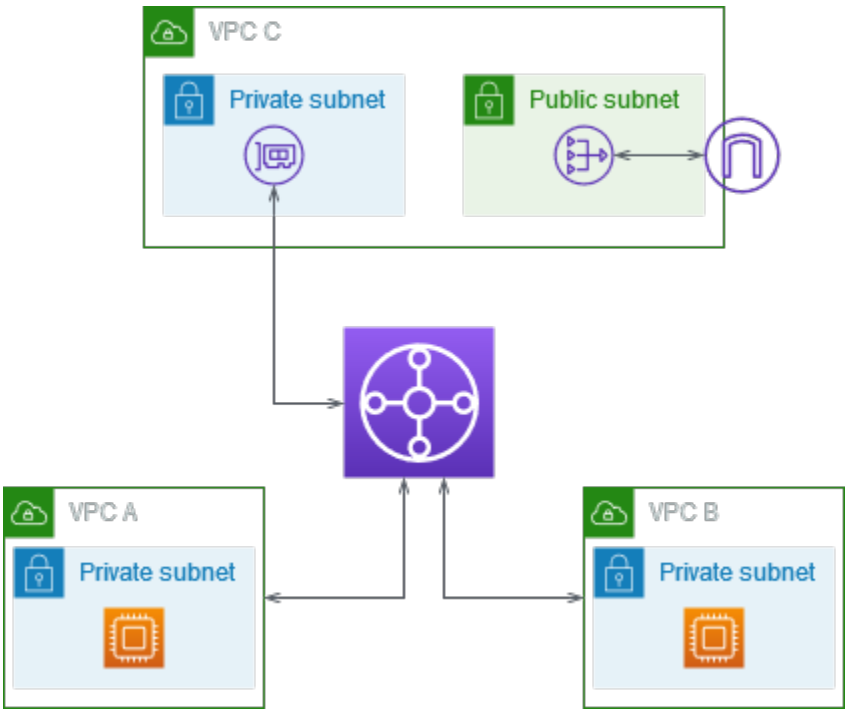
Ejemplo: enrutamiento saliente centralizado a Internet

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

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. Connect all VPCs to a una pasarela 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 VPCs 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.
- Cada una de las VPC A y VPC B tiene 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 IPv4 subred a la puerta de enlace 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 todo el resto del tráfico de IPv4 subred a la puerta de enlace 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. La entrada restante enruta todo el resto del tráfico de IPv4 subred 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*
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 enruta el resto del tráfico de IPv4 subred 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		estática

CIDR	Conexión	Tipo de ruta
	Attachment for VPC C	

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.

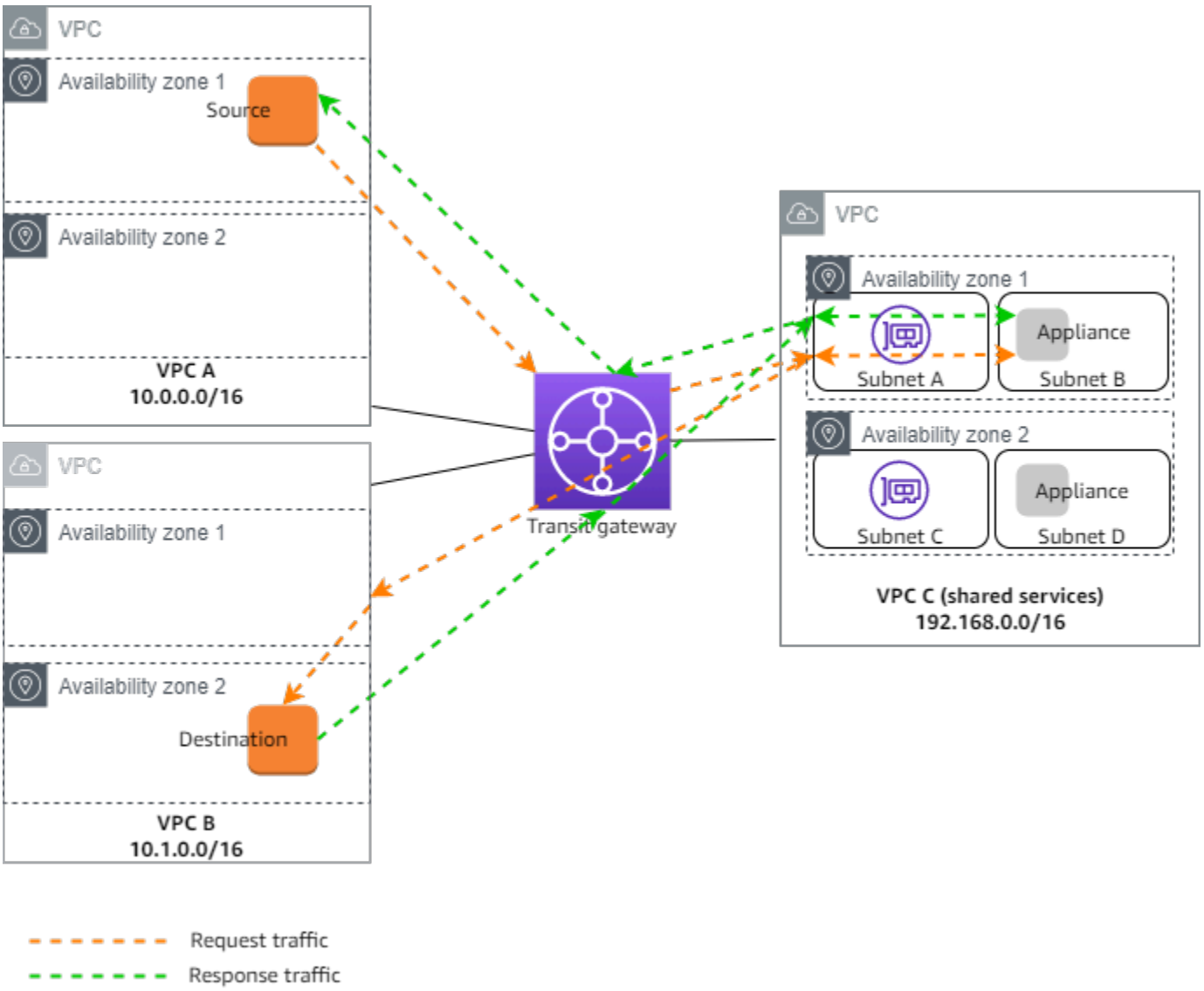
Important

- 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

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 VPCs. 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 accesorios de VPC, uno para cada uno de los. VPCs 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. AWS CloudFormation Por ejemplo, `--options ApplianceModeSupport=enable` añádalo 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

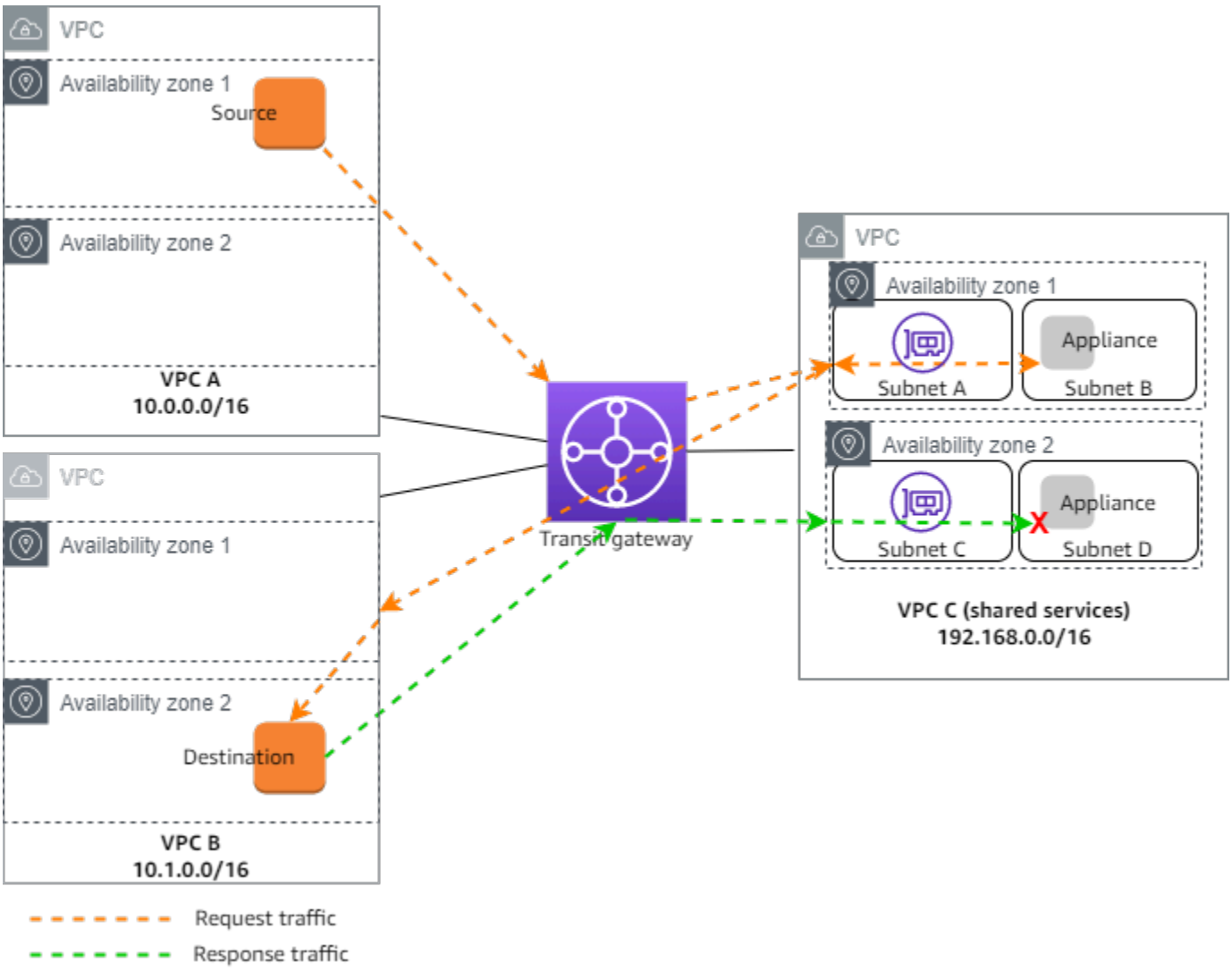
Si las conexiones de VPC abarcan varias zonas de disponibilidad y necesita que el tráfico entre hosts de origen y destino se enrute a través del mismo dispositivo para una inspección con estado, habilite la compatibilidad con el modo de dispositivo para la conexión de VPC en que se encuentra el dispositivo.

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

VPCs A y B tienen tablas de enrutamiento con 2 entradas. La primera entrada es la entrada predeterminada para el IPv4 enrutamiento local en 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 IPv4 subred a la puerta de enlace de tránsito. A continuación, se muestra la tabla de enrutamiento para VPC A.

Destino	Objetivo
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	Objetivo
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	Objetivo
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: Cómo empezar a usar Amazon VPC Transit Gateways

Los siguientes tutoriales le ayudarán a familiarizarse con las pasarelas de tránsito de Amazon VPC Transit Gateways. Las tareas de los siguientes tutoriales le ayudarán a crear una puerta de enlace de tránsito y, a continuación, a conectar dos de ellas VPCs mediante esa puerta de enlace de tránsito. Puede crear una puerta de enlace de tránsito mediante la consola de VPC de Amazon o mediante la. AWS CLI

Tareas

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

Tutorial: Creación de una AWS Transit Gateway con 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 conectar dos VPCs a ella. Creará la puerta de enlace de tránsito, conectará ambas y VPCs, a continuación, configurará las rutas necesarias para permitir la comunicación entre la puerta de enlace de tránsito y la suya VPCs.

Requisitos previos

- Para mostrar un ejemplo sencillo del uso de una pasarela de tránsito, crea dos VPCs en la misma región. No VPCs pueden ser idénticas ni superpuestas CIDRs. Lance una EC2 instancia de Amazon 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 puede haber rutas idénticas que apunten a dos rutas diferentes. VPCs Una puerta de enlace de tránsito no propaga la CIDRs de una VPC recién conectada si existe una ruta idéntica en las tablas de rutas de la puerta de enlace de tránsito.
- Compruebe que tiene los permisos necesarios para trabajar con gateways de tránsito. Para obtener más información, consulte Administración de identidades y accesos en Amazon VPC Transit Gateways .

- 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 Configurar reglas de grupos 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 la VPCs.
3. En el panel de navegación, elija Transit Gateways (Puertas de enlace 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. Debe ser el ASN del AWS lado de una sesión de Border Gateway Protocol (BGP).

        El rango va de 64512 a 65534 para 16 bits. ASNs

        El rango va de 4200000000 a 4294967294 para 32 bits. ASNs

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:
   - Soporte de DNS para conectarse a esta puerta de enlace de VPCs 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 de opciones para Configure-cross-account compartir, elige 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.
9. (Opcional) En la sección de bloques CIDR de Transit Gateway, añade un bloque CIDR de tamaño /24 o superior para IPv4 las direcciones 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 Transit Gateway se utilizan si está configurando los adjuntos de Connect (GRE) o PrivateIP. VPNs Transit Gateway asigna IPs los puntos finales del túnel (GRE/PrivateIP VPN) 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: Conecta el tuyo a tu pasarela de transporte VPCs

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 VPCs y ha lanzado una EC2 instancia en cada una, tal y como se describe enRequisitos previos.

Crear una vinculación de la puerta de enlace 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 el IPv6 soporte.
8. En VPC ID (ID de VPC), elija la VPC que desee asociar a la puerta de enlace de tránsito.
9. En Subred IDs, seleccione una subred para cada zona de disponibilidad que utilizará la puerta de enlace de tránsito 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: Agrega rutas entre la pasarela de tránsito y tu VPCs

Una tabla de rutas incluye rutas dinámicas y estáticas que determinan el siguiente salto asociado en VPCs 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

Para confirmar que la pasarela de tránsito se creó correctamente, conéctese a una EC2 instancia de Amazon en cada VPC y, a continuación, envíe datos entre ellas, por ejemplo, mediante un comando ping. Para obtener más información, consulta Connect to your EC2 instance en la Guía del EC2 usuario de Amazon.

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, asegúrate de tener:

- AWS CLI instalado y configurado con los permisos adecuados. Si no la tiene AWS CLI instalada, consulte la documentación de la interfaz de línea de AWS comandos.
- 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 EC2 instancia en cada VPC. Para conocer los pasos para lanzar una EC2 instancia en una VPC, consulte Lanzar una instancia en la Guía EC2 del usuario de Amazon.
- Grupos de seguridad configurados para permitir el tráfico ICMP entre las instancias. Para conocer los pasos para controlar el tráfico mediante grupos de seguridad, consulte Controlar el tráfico de sus AWS recursos mediante grupos de seguridad en la Guía del usuario de Amazon VPC.

- Permisos de IAM adecuados para trabajar con pasarelas de tránsito. Para comprobar los permisos de IAM de las pasarelas de tránsito, consulte Administración de identidad y acceso en las pasarelas de tránsito de Amazon VPC en la guía.AWS Transit Gateway

Pasos

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 `create-transit-gateway` solicitud en la `us-west-2` región. Se `options` incluyeron más en la solicitud. 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 pasarela de tránsito. En la respuesta, todos los `0ptions` que se devuelven son 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 su ID. Anota el ID de la pasarela de transporte público (`tgw-1234567890abcdef0`), ya que lo necesitarás en los pasos siguientes.

Paso 2: Verifica el estado de disponibilidad de la pasarela de tránsito

Cuando creas una pasarela de tránsito, se coloca en un `pending` estado. El estado pasará de estar pendiente a estar disponible automáticamente, pero hasta que no lo haga, no podrás adjuntar ninguno VPCs hasta que el estado cambie. Para verificar el estado, ejecuta el `describe-transit-gatweways` comando con el ID de Transit Gateway recién creado junto con la opción de filtros. La `filters` opción usa `Name=state` y se `Values=available` empareja. A continuación, el comando busca verificar si el estado de su pasarela de tránsito se encuentra en un estado disponible. Si es así, aparecerá la respuesta`"State": "available"`. Si se encuentra en cualquier otro estado, significa que 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: Adjunte el suyo VPCs a su pasarela de transporte

Una vez que su pasarela de transporte público esté disponible, cree un adjunto para cada VPC mediante. `create-transit-gateway-vpc-attachment` Deberás incluir el `transit-gateway-id`vpc-id, el y elsubnet-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 las teclas first `vpc_id` and: `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 el adjunto se ha adjuntado correctamente. El adjunto se crea en un `pending` estado. No es necesario cambiar este estado, ya que pasa a ser un `available` estado automáticamente. 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: `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 que el adjunto se ha adjuntado correctamente, con el adjunto actualmente en un `pending` estado.

```
{
    {
    "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: Compruebe que los archivos adjuntos de la pasarela de tránsito estén disponibles

Los adjuntos de la pasarela de tránsito se crean en un `pending` estado inicial. No podrás usar estos archivos adjuntos en tus rutas hasta que el estado cambie `aavailable`. Esto ocurre automáticamente. Utilice el `describe-transit-gateways` comando, junto con el`transit-gateway-id`, para comprobar la`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, `Values` los campos opcionales `Name` y de filtro se pasan a la solicitud:

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

La siguiente respuesta muestra que ambos archivos adjuntos están en un `available` estado:

```
{
    "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 `create-route` comando junto con la tabla de enrutamiento for `transit-gateway-id` each VPC. En el siguiente ejemplo, el comando se ejecuta dos veces, una para cada tabla de enrutamiento. La solicitud incluye la `route-table-iddestination-cidr-block`, la y `transit-gateway-id` para cada ruta de VPC que esté creando.

Para obtener más información sobre el `create-route` comando, consulte create-route.

Para la tabla de rutas 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` `destination-cidr-block` VPC diferente a la primera. Sin embargo, dado que solo utiliza una única puerta de enlace de tránsito, `transit-gateway-id` se utiliza la misma.

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

La respuesta se 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

Para confirmar que la puerta de enlace de tránsito se creó correctamente, conéctese a una EC2 instancia de una VPC, haga ping a una instancia de la otra VPC y, a continuación, ejecute el comando. `ping`

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

   ```
   ping 10.2.0.50
   ```

   > **Note**
   >
   > `10.2.0.50`Sustitúyala por la dirección IP privada real de la EC2 instancia 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 los archivos adjuntos de la pasarela de transporte y la pasarela de transporte

Cuando ya no necesites la pasarela de tránsito, puedes eliminarla. En primer lugar, debes eliminar todos los archivos adjuntos. Ejecute el `delete-transit-gateway-vpc-attachment` comando utilizando el `transit-gateway-attachment-id` para cada archivo adjunto. Después de ejecutar el comando, utilícelo `delete-transit-gateway` para eliminar la puerta de enlace de tránsito. Para lo siguiente, elimine los dos adjuntos de VPC y la puerta de enlace de tránsito única que se crearon en los pasos anteriores.

> **Important**
>
> Dejarás de incurrir en cargos una vez que elimines todos los archivos adjuntos de Transit Gateway.

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

   Para el primer archivo adjunto, ejecute el siguiente comando:

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

   La respuesta de eliminación del primer adjunto 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 `delete-transit-gateway-vpc-attachment` comando para el segundo adjunto:

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

   La respuesta de eliminación del segundo adjunto 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. Los archivos adjuntos permanecen en un `deleting` estado hasta que se eliminan. Una vez eliminados, podrás eliminar la pasarela de tránsito. Utilice el `delete-transit-gateway` comando junto con`transit-gateway-id`. Para obtener más información sobre `delete-transit-gateway` el comando, consulte delete-transit-gateway.

   En el siguiente ejemplo, `My Transit Gateway` se elimina lo que 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 el ID de la pasarela de tránsito eliminados, junto con las opciones originales definidas para la pasarela 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

Creaste correctamente una pasarela de tránsito, le conectaste dos VPCs , configuraste el enrutamiento entre ellas y verificaste la conectividad. Este sencillo ejemplo demuestra la funcionalidad básica de Amazon VPC Transit Gateways. Para situaciones más complejas, como conectarse a redes locales o implementar configuraciones de enrutamiento más avanzadas, consulte la Guía del usuario de Amazon VPC Transit Gateways.

Prácticas recomendadas de diseño de Amazon VPC Transit Gateways

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. Para cada subred, utilice un CIDR pequeño, por ejemplo/28, de modo que tenga más direcciones para EC2 los recursos. Cuando utilice una subred independiente, puede configurar los siguientes recursos:
  - Mantenga abierta la red entrante y saliente ACLs asociada a las subredes de la puerta de enlace de tránsito.
  - Según el flujo de tráfico, puede aplicar la red ACLs 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 las conexiones Site-to-Site VPN del Border Gateway Protocol (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 los adjuntos de la AWS Direct Connect puerta de enlace y los adjuntos de la Site-to-Site VPN BGP.
- 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 ambos VPCs al mismo tiempo para evitar que los paquetes gigantes se caigan debido a discordancias de 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 la AWS Transit Gateway interconexión entre regiones.

Trabajo con puertas de enlace de tránsito con Amazon VPC Transit Gateways

Puede usar puerta de enlaces de tránsito mediante la consola de Amazon VPC o la AWS CLI.

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 tablas de rutas de Transit Gateway, Transit Gateway Adjuntos y Transit Gateway APIs.

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`.
- Ejecute las APIs que crean y describen los archivos adjuntos, por ejemplo`DescribeTransitGatewayVpcAttachments`, `CreateTransitGatewayVpcAttachment` y, en sus VPCs.
- 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.

Puertas de enlace de tránsito en Amazon VPC Transit Gateways

Una pasarela de tránsito le 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 Una vez que compartes 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 público 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. 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 IPv4 o varios 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 los bloques IPv6 CIDR IPv4 y los bloques CIDR, consulte el direccionamiento IP en la Guía del usuario de Amazon VPC.

Tareas

- Creación de una puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Consulta de información de la puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Adición o edición de las etiquetas de la puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Modificación de una puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Aceptación del uso compartido de un recurso con Amazon VPC Transit Gateways
- Aceptación de una conexión compartida con Amazon VPC Transit Gateways
- Eliminación de una puerta de enlace de tránsito con Amazon VPC Transit Gateways

Creación de una puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 ???.

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 es de 64512 a 65534 para 16 bits. ASNs

El rango es de 4200000000 a 4294967294 para 32 bits. ASNs

Si tiene una implementación en varias regiones, recomendamos que utilice un ASN único para cada una de las puerta de enlaces de tránsito.

7. Para obtener compatibilidad con DNS, seleccione esta opción si necesita que la VPC resuelva los nombres de host de IPv4 DNS públicos en IPv4 direcciones privadas cuando se consultan desde instancias de otra VPC conectada a la puerta de enlace de tránsito.
8. Para admitir la referencia a grupos de seguridad, habilite esta función para hacer referencia a un grupo de seguridad VPCs conectado a una 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 lo mismo CIDRs, el tráfico se distribuye equitativamente entre ellas.

   Al seleccionar esta opción, el BGP ASN anunciado, los atributos de BGP como AS-path deben ser 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 para Configure-cross-account compartir, elige 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) Para los bloques CIDR de Transit Gateway, especifique uno IPv4 o más bloques IPv6 CIDR para su pasarela de tránsito.

    Puede especificar un bloque CIDR de tamaño /24 o superior (por ejemplo, /23 o /22) o un bloque CIDR de tamaño /64 o superior (por ejemplo IPv4, /63 o /62) para. 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 Transit Gateway se utilizan si está configurando los adjuntos de Connect (GRE) o PrivateIP. VPNs Transit Gateway asigna IPs los puntos finales del túnel (GRE/PrivateIP 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.

Consulta de información de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 pasarela de transporte público se muestran debajo de la lista de pasarelas de la página.

Para ver una pasarela de transporte público mediante el AWS CLI

Utilice el comando describe-transit-gateways.

Adición o edición de las etiquetas de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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, consulta Cómo etiquetar tus EC2 recursos de Amazon.

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 Guardar.

Modificación de una puerta de enlace de tránsito con Amazon VPC Transit Gateways

Puede modificar las opciones de configuración de una pasarela de tránsito. Cuando modificas una pasarela de transporte público, las pasarelas de transporte adjuntas existentes no sufren ninguna interrupción en el 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.

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 tu pasarela de transporte público mediante el AWS CLI

Utilice el comando modify-transit-gateway.

Aceptación del uso compartido de un recurso con Amazon VPC Transit Gateways

Si le han añadido a un recurso compartido, recibirá una invitación para unirse a este. Para poder obtener acceso a los recursos compartidos, antes debe aceptar el uso compartido del recurso.

Para aceptar el uso compartido de un recurso

1. Abra 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.

Aceptación de una conexión compartida con Amazon VPC Transit Gateways

Si no activó la función de aceptación automática de archivos adjuntos compartidos al crear su pasarela de transporte, debe aceptar manualmente los archivos adjuntos entre cuentas (compartidos) mediante la consola de Amazon VPC o la AWS CLI.

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 un archivo adjunto compartido mediante la AWS CLI

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

Eliminación de una puerta de enlace de tránsito con Amazon VPC Transit Gateways

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.

Conexiones de Amazon VPC en Amazon VPC Transit Gateways

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. Al especificar una subred de una zona de disponibilidad, se permite que el tráfico llegue a los recursos de todas las subredes de dicha zona.

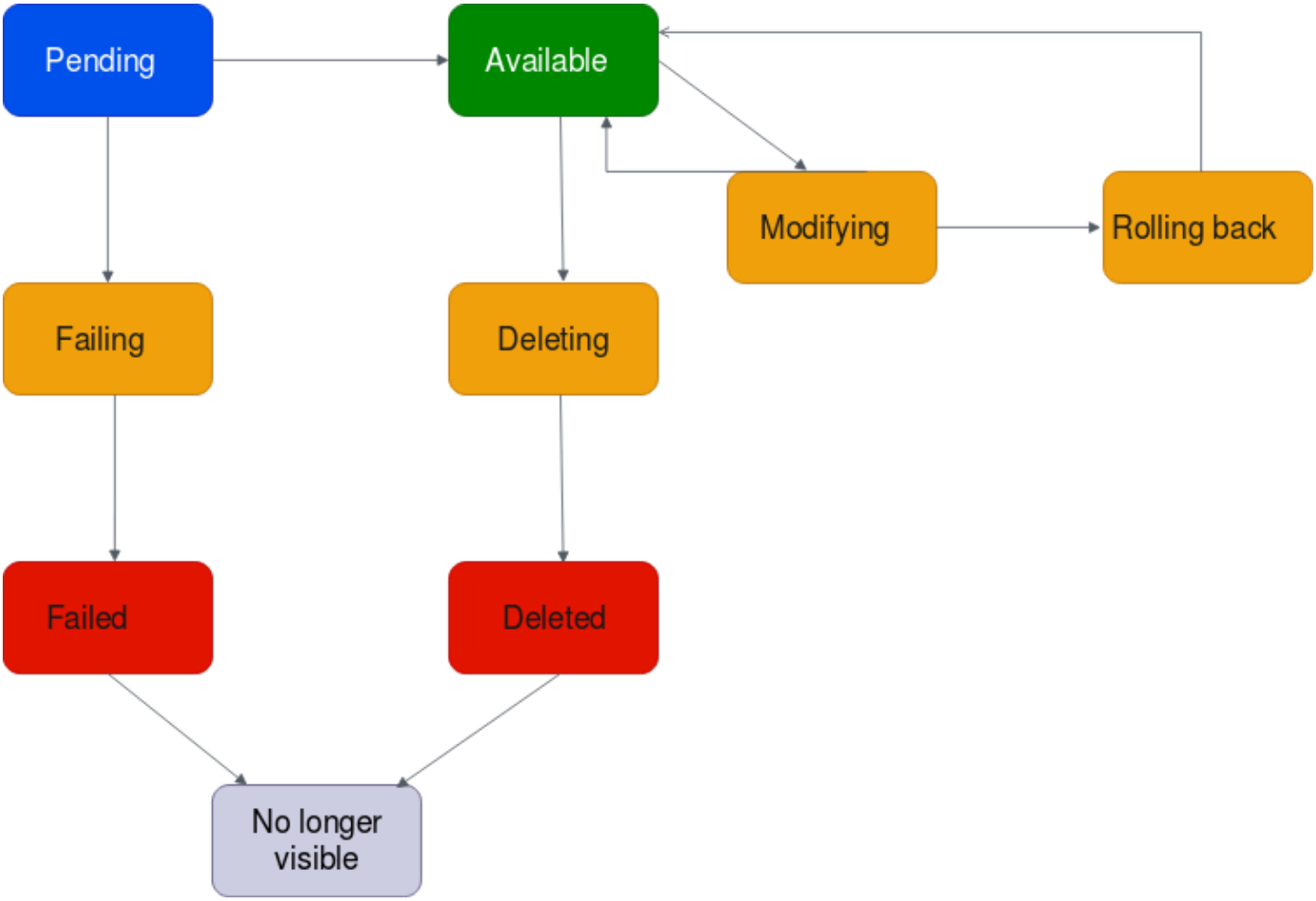
Límites

- 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. 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 la puerta de enlace de tránsito tenga una conexión en una subred en la misma zona de disponibilidad.
- 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 conecta una VPC a una puerta de enlace de tránsito y su CIDR es idéntica o se superpone con la CIDR de otra VPC que ya está conectada a la puerta de enlace de tránsito, las rutas de la VPC recién conectada no se propagan a la tabla de rutas 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.

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.

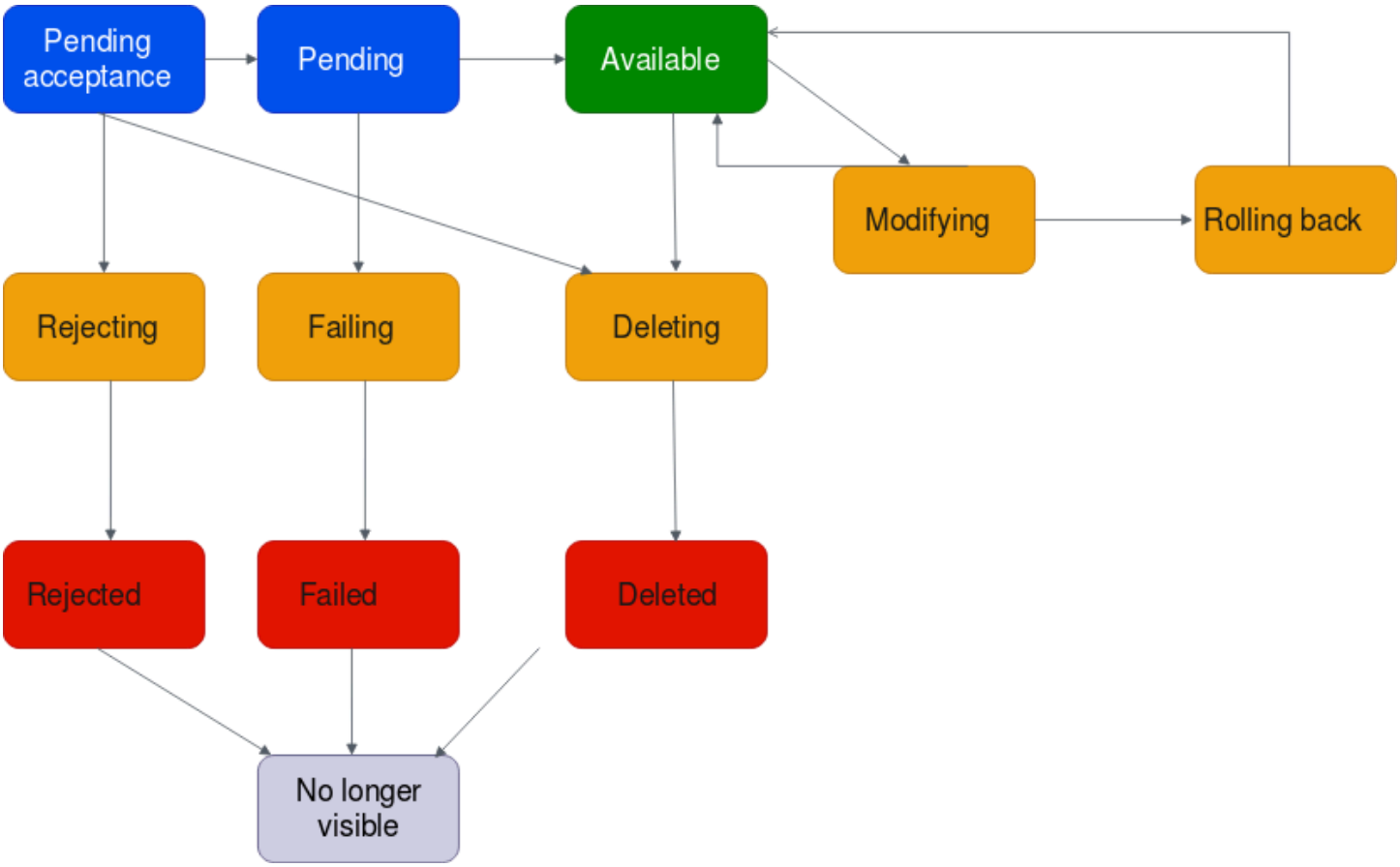
El siguiente diagrama muestra los estados por los que puede pasar una conexión en una única configuración de cuenta, o una configuración entre cuentas que tenga activada la opción Aceptar automáticamente las conexiones compartidas .



- 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 planea configurar un dispositivo de red con estado en su VPC, puede habilitar la compatibilidad con el modo dispositivo para el adjunto de VPC en el que se encuentra el dispositivo al crear un adjunto. 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 que haya una asociación de subred en esa zona. Si bien el modo dispositivo solo se admite en los adjuntos de VPC, el flujo de red puede provenir de cualquier otro tipo de adjunto de Transit Gateway, incluidos los adjuntos de VPC, VPN y Connect. El modo dispositivo

también funciona para flujos de red que tienen orígenes y destinos 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 los archivos adjuntos para habilitarlo. Puede activar o desactivar el modo dispositivo mediante la consola, la línea de comandos o la API.

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 según la configuración específica y los patrones de tráfico. Los siguientes son ejemplos de escenarios.

Escenario 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 adjuntos de VPC en modo dispositivo tanto en us-east-1a como en us-east-1b, Transit Gateway 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.

Escenario 2: Enrutamiento del tráfico entre zonas de disponibilidad a través de la VPC del dispositivo

Para el tráfico que fluye desde la zona de disponibilidad de origen us-east-1a a la zona de disponibilidad de destino us-east-1b, con adjuntos de VPC en modo dispositivo tanto en us-east-1a como en us-east-1b, Transit Gateway utiliza un algoritmo de hash de flujo para seleccionar us-east-1a o us-east-1b en la VPC del dispositivo. La zona de disponibilidad elegida se utiliza de forma coherente durante toda la vida útil del flujo.

Escenario 3: enrutamiento del tráfico a través de una VPC de dispositivo sin datos de zona de disponibilidad

Cuando el tráfico se origina desde la zona de disponibilidad us-east-1a de origen hacia un destino sin información sobre la zona de disponibilidad (por ejemplo, tráfico con destino a Internet), con adjuntos de VPC en modo dispositivo tanto en us-east-1a como en us-east-1b, Transit Gateway selecciona una interfaz de red de us-east-1a dentro de la VPC del dispositivo.

Escenario 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 adjuntos de VPC en modo dispositivo en distintas zonas de disponibilidad, por ejemplo us-east-1c y us-east-1d, Transit Gateway utiliza 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 toda la vida útil del flujo.

> **Note**
>
> El modo dispositivo solo se admite para los adjuntos de VPC. Asegúrese de que la propagación de rutas esté habilitada para una tabla de enrutamiento asociada a un adjunto 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 VPCs que atraviese los grupos 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.

El soporte de referencia a grupos de seguridad se puede configurar tanto para las puertas de enlace de tránsito como para los adjuntos de VPC de las puertas de enlace de tránsito y solo funcionará si se ha habilitado tanto para una puerta de enlace de tránsito como para sus adjuntos de VPC.

Limitaciones

Se aplican las siguientes limitaciones cuando se utiliza la referencia a grupos de seguridad con un adjunto de VPC.

- No se admite la referencia a grupos de seguridad en las conexiones de interconexión de Transit Gateway. Ambas VPCs deben estar conectadas a la misma puerta de enlace 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 basadas en el CIDR IP.
- 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

- Creación de una conexión de VPC con Amazon VPC Transit Gateways
- Modificación de una conexión de la VPC con Amazon VPC Transit Gateways
- Modificación de las etiquetas de vinculaciones de la VPC con Amazon VPC Transit Gateways
- Consulta de una conexión de VPC con Amazon VPC Transit Gateways
- Eliminación de una vinculación de VPC con Amazon VPC Transit Gateways
- Actualizar las reglas de entrada de los grupos de AWS Transit Gateway seguridad
- Identificar los grupos de seguridad AWS Transit Gateway referenciados
- Eliminar reglas de grupos AWS Transit Gateway de seguridad obsoletas
- Solución de problemas con la creación de conexiones de VPC en Amazon VPC Transit Gateways

Creación de una conexión de VPC con Amazon VPC Transit Gateways

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. Elija si desea habilitar la compatibilidad con los modos DNS IPv6 Support, Support y Appliance.

   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. Active esta función para hacer referencia a un grupo de seguridad VPCs conectado a una 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. Elija si desea activar IPv6Support.
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 Subred IDs, seleccione una subred para cada zona de disponibilidad que utilizará la puerta de enlace de tránsito 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 un adjunto de VPC mediante el AWS CLI

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

Modificación de una conexión de la VPC con Amazon VPC Transit Gateways

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 apoyo
   - 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 con Amazon VPC Transit Gateways

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 Guardar.

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

Consulta de una conexión de VPC con Amazon VPC Transit Gateways

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 los archivos adjuntos de la VPC mediante el AWS CLI

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

Eliminación de una vinculación de VPC con Amazon VPC Transit Gateways

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 un adjunto de VPC mediante el AWS CLI

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

Actualizar las reglas de entrada de los grupos de AWS Transit Gateway seguridad

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 Security Groups (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)

Identificar los grupos de seguridad AWS Transit Gateway referenciados

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)

Eliminar reglas de grupos AWS Transit Gateway de seguridad obsoletas

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 que haya identificado las reglas anticuadas del grupo de seguridad, puede eliminarlas mediante los comandos revoke-security-group-ingresso revoke-security-group-egress.

Solución de problemas con la creación de conexiones de VPC en Amazon VPC Transit Gateways

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 debido a que hay demasiadas solicitudes de IAM; por ejemplo, está utilizando AWS 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 el adjunto 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”.

AWS Adjuntos de funciones de red Transit Gateway

Puedes crear un accesorio de función de red al que conectar directamente tu pasarela de transporte AWS Network Firewall. Esto elimina la necesidad de crear y gestionar la inspección VPCs.

Con un firewall adjunto, aprovisiona y administra AWS automáticamente todos los recursos necesarios entre bastidores. Verás un nuevo adjunto a la pasarela de tránsito en lugar de puntos finales de firewall individuales. Esto simplifica el proceso de implementación de la inspección centralizada del tráfico de la red.

Antes de poder utilizar un accesorio de firewall, primero debe crearlo en AWS Network Firewall. Para conocer los pasos necesarios para crear el adjunto, consulte Introducción a la AWS Network Firewall administración en la Guía para AWS Network Firewall desarrolladores Una vez creado el firewall, podrá ver el adjunto en la consola de Transit Gateway, en la sección Adjuntos. El archivo adjunto 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 pasarela de tránsito y alguien ha creado un firewall adjunto a su pasarela de tránsito desde otra cuenta, debe aceptar o rechazar la solicitud de adjunto.

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.

Acepte o rechace un adjunto a una función de red mediante la consola

Utilice la consola de Amazon VPC para aceptar o rechazar un adjunto a una función de red de Transit Gateway.

Para aceptar o rechazar un adjunto a una 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, elija Transit Gateways.
3. Selecciona los archivos adjuntos de Transit Gateway.
4. Seleccione el archivo adjunto con el estado Pendiente de aceptación y un tipo de función de red.
5. Seleccione Acciones y, a continuación, elija Aceptar adjunto o Rechazar adjunto.
6. En el cuadro de diálogo de confirmación, seleccione Aceptar o Rechazar.

Si acepta el archivo adjunto, se activa y el firewall puede inspeccionar el tráfico. Si rechaza el archivo adjunto, 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.

Vea un adjunto a una función de red mediante la consola de Network Manager

Puede ver los adjuntos de una función de red mediante la consola de Network Manager.

Para ver los archivos adjuntos 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 aún no tiene una.
3. Registre su pasarela de tránsito en Network Manager.
4. En Redes globales, elige la red global en la que se encuentra el adjunto.
5. En el panel de navegación, seleccione Transit gateways (Puertas de enlace de tránsito).
6. Elija la pasarela de transporte de la que desee ver los archivos adjuntos.
7. Elija la vista en árbol topológico. Los archivos adjuntos de Network Firewall aparecen con un icono de función de red.
8. Para ver los detalles sobre un accesorio de firewall específico, 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 los archivos adjuntos del firewall, incluido su estado, la puerta de enlace de tránsito asociada y las zonas de disponibilidad.

Ver un adjunto de función de red mediante la consola de Amazon VPC

Usa la consola de VPC para ver una lista de los tipos de adjuntos de tu pasarela de tránsito.

Para ver los tipos de adjuntos de Transit Gateway 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 un adjunto de función de red, debe actualizar las tablas de rutas de Transit Gateway 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 la asociación de una tabla de rutas de una pasarela de tránsito, consulteAsociar una tabla de enrutamiento de la puerta de enlace de tránsito.

Dirija el tráfico a través de un servidor de seguridad adjunto mediante la consola

Utilice la consola de Amazon VPC Console para enrutar el tráfico a través de un adjunto de función de red de Transit Gateway.

Para enrutar el tráfico a través de un accesorio 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, elija Transit Gateways.
3. Elija las tablas de rutas de Transit Gateway.
4. Seleccione la tabla de rutas que desee modificar.
5. Elija Acciones y, a continuación, elija Crear ruta estática.
6. Para CIDR, introduzca el bloque CIDR de destino para la ruta.
7. En Adjunto, seleccione el adjunto de la 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 rutas estáticas.

El tráfico que coincida con el bloque CIDR de su tabla de rutas ahora se enviará al archivo adjunto del firewall para su inspección antes de reenviarlo a su destino final.

Enrute el tráfico a través de un adjunto de función de red mediante la CLI o la API

Utilice la línea de comandos o la API para enrutar un adjunto a una función de red de una pasarela de tránsito.

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

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

  Por ejemplo, la solicitud podría ser para enrutar un adjunto 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
```

  A continuación, 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 CIDR de su tabla de enrutamiento ahora se enviará al archivo adjunto del firewall para su inspección antes de reenviarse a su destino final.

AWS Site-to-Site VPN archivos adjuntos en Amazon VPC Transit Gateways

Puede conectar un adjunto de Site-to-Site VPN a una puerta de enlace de tránsito en Amazon VPC Transit Gateways, lo que le permitirá conectar sus redes VPCs y las locales. Se admiten rutas dinámicas y estáticas, así como y. IPv4 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, revise los requisitos de la puerta de enlace del cliente para asegurarse 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.
- En el caso de la estática VPNs, también tendrás que añadir primero las rutas estáticas a la tabla de rutas de la pasarela 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 Site-to-Site VPN, ya que esto podría

permitir un flujo de tráfico saliente no deseado cuando se utiliza una VPN basada en BGP. 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

- Creación de una conexión de puerta de enlace de tránsito a una VPN con Amazon VPC Transit Gateways
- Consulta de una conexión de VPN con Amazon VPC Transit Gateways
- Eliminación de una vinculación de VPN con Amazon VPC Transit Gateways

Creación de una conexión de puerta de enlace de tránsito a una VPN con Amazon VPC Transit Gateways

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 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.

- 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 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.

Consulta de una conexión de VPN con Amazon VPC Transit Gateways

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.

Eliminación de una vinculación de VPN con Amazon VPC Transit Gateways

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 archivo adjunto de VPN mediante el AWS CLI

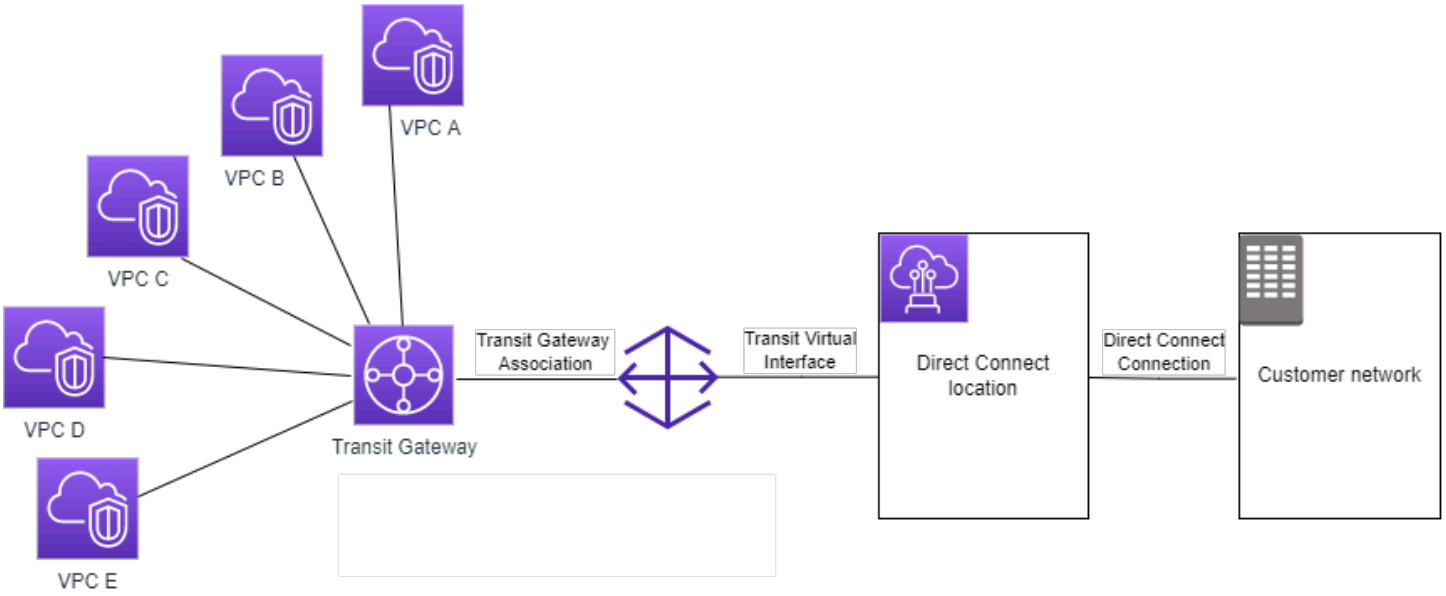
Utilice el comando delete-vpn-connection.

Conexiones de puerta de enlace de tránsito a una puerta de enlace de Direct Connect en Amazon VPC Transit Gateways

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:

- Administre una sola conexión para varias VPCs o VPNs que estén en la misma región.
- Anuncie prefijos desde las instalaciones locales hacia AWS y desde AWS las instalaciones locales.

El siguiente diagrama ilustra cómo la puerta de enlace Direct Connect le permite crear una única conexión a su conexión Direct Connect que todos VPCs pueden usar.



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 Amazon VPC Transit Gateways

Puede emparejar pasarelas de tránsito intrarregionales e interregionales y enrutar el tráfico entre ellas, lo que incluye IPv4 el tráfico. 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 pasarela de tránsito entre pares puede estar en tu cuenta o puede provenir de otra cuenta. También puedes solicitar un archivo adjunto de interconexión desde tu propia cuenta a una pasarela 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.

Recomendamos utilizar una puerta de enlace de tránsito única ASNs para cada par a fin de aprovechar las capacidades de propagación de rutas futuras.

La interconexión de la puerta de enlace de tránsito no permite convertir nombres de host IPv4 DNS públicos o privados en IPv4 direcciones privadas a ambos VPCs lados del archivo adjunto de interconexión de la pasarela de tránsito utilizando la Amazon Route 53 Resolver de 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 se cifra doblemente en los enlaces de red que están fuera del control físico de los mismos. 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 los archivos adjuntos de interconexión entre pasarelas de tránsito, consulte AWS Transit Gateways FAQs.

Consideraciones sobre la opción regional de suscripción AWS

Puede interconectar las puerta de enlaces de tránsito a través de los límites de la región registrada. Para obtener información sobre estas regiones y sobre cómo suscribirse a ellas, consulte Administración de AWS regiones. 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 suscripción de la región, AWS comparte los siguientes datos de cuenta con la cuenta que acepta la conexión entre pares:
  - Cuenta de AWS ID
  - 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 con Amazon VPC Transit Gateways
- Aceptación o rechazo de una solicitud de vinculación de interconexión con Amazon VPC Transit Gateways

- Adición de una ruta a la tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Eliminación de una vinculación de interconexión con Amazon VPC Transit Gateways

Creación de una vinculación de interconexión con Amazon VPC Transit Gateways

Antes de empezar, asegúrese de que tiene el ID de la puerta de enlace de tránsito que desea asociar. Si la pasarela de tránsito está en otra Cuenta de AWS, asegúrese de tener el Cuenta de AWS ID del propietario de la pasarela de tránsito.

Después de crear la interconexión, el propietario de la puerta de enlace de tránsito del aceptador debe aceptar 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 pasarela de transporte está en otra Cuenta de AWS, selecciona 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 un archivo adjunto de interconexión mediante AWS CLI

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

Aceptación o rechazo de una solicitud de vinculación de interconexión con Amazon VPC Transit Gateways

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. Esto es necesario incluso si ambas puerta de enlaces de tránsito están en la misma cuenta. La vinculación de interconexión de estar en el estado `pendingAcceptance`. Acepte la solicitud de vinculación de interconexión de la región en la que se encuentra la puerta de enlace de tránsito del aceptador.

También puede rechazar cualquier solicitud de interconexión recibida con el estado `pendingAcceptance`. 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 un archivo adjunto de igual a igual mediante el AWS CLI

Utilice los comandos accept-transit-gateway-peering-attachment y reject-transit-gateway-peering-attachment.

Adición de una ruta a la tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 AWS CLI

Utilice el comando create-transit-gateway-route.

> **Important**
>
> Después de crear la ruta, asocie la tabla de enrutamiento de la puerta de enlace de tránsito con la interconexión 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”.

Eliminación de una vinculación de interconexión con Amazon VPC Transit Gateways

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 un adjunto de interconexión mediante el AWS CLI

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

Conecta archivos adjuntos y conecta pares en Amazon VPC Transit Gateways

Puede crear una conexión de Transit Gateway Connect para establecer una conexión entre una puerta de enlace de tránsito y dispositivos virtuales de terceros (como dispositivos SD-WAN) 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 emparejamiento 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 dispositivos SD-WAN con AWS Transit Gateway y. AWS 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 para. `169.254.0.0/16` IPv4 Si lo desea, puede especificar un bloque CIDR de /125 del rango para. `fd00::/8` 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 IPv4 rango del dispositivo como dirección IP BGP. Cuando lo utilice IPv6, si su bloque CIDR interno es fd00: :/125, debe configurar la primera dirección de este rango (fd00: :1) en la interfaz de 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 IPv6 dirección IPv4 O, pero debe ser de la misma familia de direcciones IP que la dirección de la puerta de enlace 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.

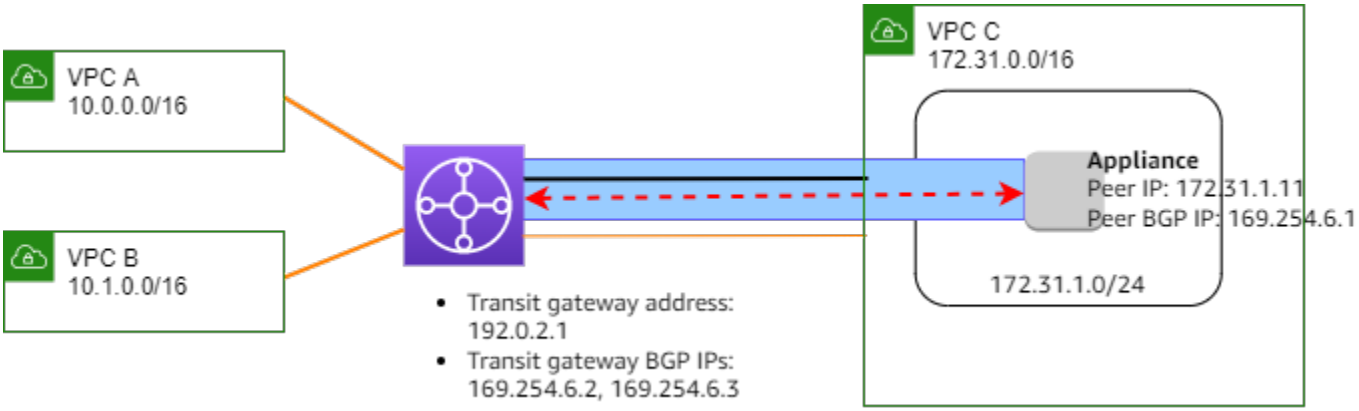
Puede agregar un bloque CIDR de gateway de tránsito cuando crea o modifica una gateway de tránsito.

La dirección IP puede ser una IPv6 dirección IPv4 O, pero debe ser de la misma familia de direcciones IP que la dirección IP del mismo nivel.

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 multiprotocolo (MP-BGP), donde se requiere el direccionamiento de unidifusión para establecer también una sesión de BGP para IPv4 Unicast. IPv6 Puede usar ambas direcciones y para las direcciones IP externas del GRE. IPv4 IPv6

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



Componente de diagrama	Descripción
	Conexión de VPC
	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	Objetivo
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 usa eBGP, debe configurar ebgp-multihop con un valor time-to-live (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 iBGP (dispositivo de terceros), a menos que las rutas se originen en un par eBGP y deban estar configuradas. next-hop-self 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 familias de direcciones. IPv4 IPv6
- El tiempo de espera predeterminado de mantenimiento BGP es de 10 segundos y el temporizador de retención predeterminado es de 30 segundos.
- IPv6 No se admite la interconexión BGP; solo se admite la interconexión BGP basada en bases. IPv4 IPv6 los prefijos se intercambian IPv4 mediante el emparejamiento BGP 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.
- Una interconexión de Connect que utilice el atributo BGP AS-PATH es la ruta preferida cuando tenga dos interconexiones de Connect.

  Para utilizar el enrutamiento de múltiples rutas de acceso de igual costo (ECMP) entre varios dispositivos, debe configurar el dispositivo para anunciar los mismos prefijos en la gateway de tránsito con el mismo atributo AS-PATH de BGP. Para que la gateway de tránsito elija todas las rutas de ECMP disponibles, el 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 (8 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 1472 bytes (1500 - 8 - 20 = 1472) para evitar la fragmentación de los paquetes.

Tareas

- Creación de una conexión de Connect con Amazon VPC Transit Gateways
- Creación de un par de Connect con Amazon VPC Transit Gateways
- Consulta de conexiones y pares de Connect con Amazon VPC Transit Gateways
- Modificación de las etiquetas de conexión y de pares de Connect con Amazon VPC Transit Gateways
- Eliminación de un par de Connect con Amazon VPC Transit Gateways
- Eliminación de una conexión de Connect con Amazon VPC Transit Gateways

Creación de una conexión de Connect con Amazon VPC Transit Gateways

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 un archivo adjunto de Connect mediante el AWS CLI

Utilice el comando create-transit-gateway-connect.

Creación de un par de Connect con Amazon VPC Transit Gateways

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. Para los bloques BGP Inside CIDR IPv4, especifique el rango de IPv4 direcciones internas que se utilizan para el emparejamiento de BGP. Especifique un bloque CIDR /29 del rango `169.254.0.0/16`.
8. (Opcional) Para los bloques BGP Inside CIDR IPv6, especifique el rango de IPv6 direcciones internas que se utilizan para la interconexión 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 mismo nivel para que sea diferente del ASN de la puerta de enlace de tránsito (eBGP), debe configurar ebgp-multihop con un valor (TTL) de 2. time-to-live
10. Elija Create Connect peer (Crear par de Connect).

Para crear un peer de Connect mediante el AWS CLI

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

Consulta de conexiones y pares de Connect con Amazon VPC Transit Gateways

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.

Modificación de las etiquetas de conexión y de pares de Connect con Amazon VPC Transit Gateways

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 Guardar.

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 Guardar.

Para modificar las etiquetas de la conexión y la interconexión de Connect mediante la AWS CLI

Utilice los comandos create-tags y delete-tags.

Eliminación de un par de Connect con Amazon VPC Transit Gateways

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 un par de Connect mediante el AWS CLI

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

Eliminación de una conexión de Connect con Amazon VPC Transit Gateways

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 un archivo adjunto de Connect mediante el AWS CLI

Utilice el comando delete-transit-gateway-connect.

Tablas de enrutamiento de la puerta de enlace de tránsito en Amazon VPC Transit Gateways

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 red entre su VPCs y VPNs. 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. Las conexiones de VPC, VPN, puerta de enlace de Direct Connect, interconexión y Connect son todas compatibles. 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

- Creación de una tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Consulta de tablas de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

Creación de una tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 rutas de la puerta de enlace de tránsito mediante el AWS CLI

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

Consulta de tablas de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 su puerta de enlace de transporte mediante 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.

Asociación de una tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 Crear asociación.
6. Elija la vinculación que se va a asociar y, a continuación, elija Create association (Crear asociación).

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

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

Eliminación de la asociación de una tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 puerta de enlace de tránsito mediante el AWS CLI

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

Habilitación de la propagación de rutas en la tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 Amazon VPC Transit Gateways

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 el AWS CLI

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

Creación de una ruta estática con Amazon VPC Transit Gateways

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.

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 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 mediante el AWS CLI

Utilice el comando create-transit-gateway-route.

Eliminación de una ruta estática con Amazon VPC Transit Gateways

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 mediante el AWS CLI

Utilice el comando delete-transit-gateway-route.

Reemplazo de una ruta estática con Amazon VPC Transit Gateways

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 el AWS CLI

Utilice el comando replace-transit-gateway-route.

Exportación de las tablas de enrutamiento a Amazon S3 con Amazon VPC Transit Gateways

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 navegue hasta el bucket que especificó. El nombre del archivo incluye el Cuenta de AWS ID, la AWS región, el ID de la tabla de rutas y una marca de tiempo. 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"
    }
  ]
}
```

Eliminación de una tabla de enrutamiento de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 rutas de una puerta de enlace de tránsito mediante el AWS CLI

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

Creación de una referencia de lista de prefijos para la tabla de enrutamiento con Amazon VPC Transit Gateways

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 especificas con frecuencia el mismo destino CIDRs en varias tablas de rutas de Transit Gateway, puedes administrarlos CIDRs en una sola lista de prefijos, en lugar de hacer referencia repetidamente al mismo CIDRs en cada tabla de rutas. 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 a una lista de prefijos mediante el AWS CLI

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

Modificación de una referencia de lista de prefijos con Amazon VPC Transit Gateways

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 a una lista de prefijos mediante el AWS CLI

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

Eliminación de una referencia de lista de prefijos con Amazon VPC Transit Gateways

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 a una lista de prefijos mediante el AWS CLI

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

Tablas de políticas de la puerta de enlace de tránsito en Amazon VPC Transit Gateways

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

- Creación de una tabla de políticas para la puerta de enlace de tránsito con Amazon VPC Transit Gateways
- Eliminación de una tabla de políticas de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

Creación de una tabla de políticas para la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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.

Eliminación de una tabla de políticas de la puerta de enlace de tránsito con Amazon VPC Transit Gateways

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 Amazon VPC Transit Gateways

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 las subredes conectadas VPCs y sirve como enrutador de multidifusión para las instancias que envían tráfico destinado a varias instancias de recepción.

Temas

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 mediante interfaces de red elásticas individuales conectadas a las 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 IGMPv2 protocolo y los dominios de multidifusión que pertenecen a grupos IGMP y estáticos (basados en API).

- Fuente de multidifusión: interfaz de red elástica asociada a una EC2 instancia 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. Se usa AWS CLI para agregar una fuente y miembros de un grupo. El origen agregado estáticamente envía tráfico de multidifusión y los miembros reciben tráfico de multidifusión.
- Miembro de un grupo de multidifusión: interfaz de red elástica asociada a una EC2 instancia 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 Transit Gateway puede no ser adecuada para operaciones de alta frecuencia o aplicaciones sensibles al rendimiento. Te recomendamos encarecidamente que revises las cuotas de multidifusión para conocer los límites. Póngase en contacto con su cuenta o con el equipo de arquitectos de soluciones para obtener una revisión detallada de sus requisitos de rendimiento.
- Para obtener información sobre las regiones compatibles, consulte AWS Transit Gateway FAQs.
- Debe crear una nueva puerta de enlace de tránsito para admitir la multidifusión.
- La pertenencia a un grupo de multidifusión se gestiona mediante el IGMP Amazon Virtual Private Cloud Console o AWS CLI 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 deshabilitar la comprobación, consulta Cambiar la comprobación de origen o destino en la Guía del EC2 usuario de Amazon.
- Una instancia que no sea Nitro no puede ser remitente de multidifusión.
- No se admite el enrutamiento de multidifusión a través de Site-to-Site VPN AWS Direct Connect, los archivos adjuntos de peering o los archivos adjuntos 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)..
- Al inicio, un host IGMP envía varios IGMP JOIN mensajes para unirse a un grupo de multidifusión (normalmente de 2 a 3 reintentos). En el improbable caso de que todos los IGMP JOIN si se pierden los mensajes, el host no pasará a formar parte del grupo de multidifusión de Transit Gateway. En tal escenario, tendrá que volver a activar el IGMP JOIN mensaje del anfitrión utilizando métodos específicos de la aplicación.
- La pertenencia a un grupo comienza con la recepción de IGMPv2 JOIN mensaje por parte de la pasarela de tránsito y finaliza con la recepción del IGMPv2 LEAVE "Hello, World!". 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 pasarela de tránsito emite un IGMPv2 QUERY envía un mensaje a todos los miembros cada dos minutos. Cada miembro envía un IGMPv2 JOIN mensaje de respuesta, que es la forma en que los miembros renuevan su membresía. 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 su to-be-queried lista. Un explícito IGMPv2 LEAVE el mensaje elimina de forma inmediata y permanente el host de cualquier procesamiento de multidifusión posterior.
- La puerta de enlace de tránsito realiza un seguimiento de los hosts que se unieron correctamente al grupo. En caso de que se interrumpa la puerta de enlace de tránsito, la puerta de enlace de tránsito continúa enviando datos de multidifusión al host durante siete minutos (420 segundos) después del último IGMP correcto JOIN "Hello, World!". La pasarela de tránsito sigue enviando consultas de membresía al anfitrión durante un máximo de 12 horas o hasta que reciba un IGMP LEAVE mensaje del anfitrión.
- 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 hosts (instancias) IGMP y cualquier ACLs configuración en las subredes del 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, Amazon VPC Transit Gateways elimina automáticamente los grupos y fuentes estáticos que ya no ENIs existen. Esto se realiza asumiendo periódicamente la función vinculada al servicio Transit Gateway que se describe ENIs en la cuenta.
- Solo admite la multidifusión estática. 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.

Red ACLs

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 Red ACLs 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

Tipo	Protocolo	Destino	Descripción
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 Amazon VPC Transit Gateways

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 soporte (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)	Este atributo determina si hay orígenes de multidifusión estáticos para el grupo. Cuando este atributo está habilitado, debe agregar fuentes para un dominio de multidifusión mediante register-transit-gateway-

Atributo	Descripción
Static sources support (Compatibilidad con fuentes estáticas) (consola)	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 en subredes asociadas al dominio de multidifusión puede enviar tráfico de multidifusión y los miembros del grupo reciben el tráfico de multidifusión.

Creación de un dominio de multidifusión de IGMP con Amazon VPC Transit Gateways

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 Amazon VPC Transit Gateways

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. Para obtener IGMPv2 asistencia, desactive 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 estático 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=enable,Igmpv2Support=disable
```

Asociación de conexiones y subredes de VPC con un dominio de multidifusión con Amazon VPC Transit Gateways

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 Conexiones de Amazon VPC en Amazon VPC Transit Gateways.

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.

Desasociación de una subred de un dominio de multidifusión con Amazon VPC Transit Gateways

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 puerta de enlace 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 disociar subredes mediante el AWS CLI

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

Consulta de asociaciones de dominios de multidifusión en Amazon VPC Transit Gateways

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 el AWS CLI

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

Agregado de etiquetas a un dominio de multidifusión con Amazon VPC Transit Gateways

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, consulta Cómo etiquetar tus EC2 recursos de Amazon.

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 puerta de enlace 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 añadir etiquetas a un dominio de multidifusión mediante el AWS CLI

Utilice el comando create-tags.

Eliminación de un dominio de multidifusión con Amazon VPC Transit Gateways

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 puerta de enlace 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 AWS CLI

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

Dominios de multidifusión compartidos en Amazon VPC Transit Gateways

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, debe ser el propietario de ese dominio en su 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.

Uso compartido de recursos entre zonas de disponibilidad en Amazon VPC Transit Gateways

Para garantizar que los recursos se distribuyen por todas las zonas de disponibilidad de una región, Amazon VPC Transit Gateways asigna zonas de disponibilidad a nombres de cada cuenta de manera independiente. 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.

Uso compartido de un dominio de multidifusión con Amazon VPC Transit Gateways

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 uso compartido de recursos 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 que sea de su propiedad mediante AWS CLI

Utilice el comando create-resource-share.

Detención del uso compartido de dominios de multidifusión con Amazon VPC Transit Gateways

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

Para dejar de compartir un dominio de multidifusión compartido que sea de tu propiedad mediante AWS CLI

Utilice el comando disassociate-resource-share.

Identificación de un dominio de multidifusión compartido con Amazon VPC Transit Gateways

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.

Registro de orígenes con un grupo de multidifusión con Amazon VPC Transit Gateways

> **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
- Las IDs 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.

Registro de miembros con un grupo de multidifusión con Amazon VPC Transit Gateways

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 IDs interfaces 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 los orígenes de un grupo de multidifusión con Amazon VPC Transit Gateways

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 puerta de enlace 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 una fuente mediante el AWS CLI

Utilice el comando deregister-transit-gateway-multicast-group-sources.

Anulación del registro de miembros a un grupo de multidifusión con Amazon VPC Transit Gateways

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.

Consulta de grupos de multidifusión en Amazon VPC Transit Gateways

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 Amazon VPC Transit Gateways

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 configurar esto PowerShell, necesitará usar y ejecutar los siguientes comandos:

Para configurar la multidifusión para Windows Server mediante PowerShell

1. Cambie Windows Server para usarlo 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. Reinicia la EC2 instancia.
5. Pruebe su aplicación de multidifusión para asegurarse de que el tráfico fluya según lo esperado.

Ejemplo: administración de configuraciones de IGMP con Amazon VPC Transit Gateways

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 agregar de forma estática hosts que no sean IGMP como miembros de un grupo mediante. 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: administración de configuraciones de origen estático con Amazon VPC Transit Gateways

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:

   - Deshabilite el soporteIGMPv2 .
   - 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: Administración de las configuraciones de miembros de grupos estáticos en Amazon VPC Transit Gateways

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:

- Deshabilite el soporteIGMPv2 .
- 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”.

Registros de flujo de Amazon VPC Transit Gateways

Los registros de flujo de Transit Gateway son una característica de Amazon VPC Transit Gateways que permite capturar información sobre el tráfico IP que entra y sale de sus puertas de enlace 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”. Si desea capturar información sobre el tráfico IP que entra y sale de las interfaces de red de su empresa VPCs, utilice los registros de flujo de 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 (en el caso de los CloudWatch registros) ni ningún objeto de archivo de registro (en el caso de Amazon S3) existente en 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 Eliminación de una entrada de registro de flujo de Amazon VPC Transit Gateways.

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 Logs CloudWatch
- Crear un registro de flujo que se publique en Amazon S3
- Crear un registro de flujo que 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.

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 plano, todos los campos son de este tipo STRING. Si el formato es Parquet, consulte la tabla para ver los tipos de datos de los campos.

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. Para 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
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.	6

Campo	Descripción	Versión
	Tipo de datos de Parquet: STRING	
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
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

Campo	Descripción	Versión
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
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

Campo	Descripción	Versión
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, consulta Elastic Fabric Adapter en la Guía del EC2 usuario de Amazon. 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
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

Campo	Descripción	Versión
packets-lost-ttl-expired	Los paquetes perdidos debido a la caducidad de time-to-live. Tipo de datos de Parquet: INT_64	6
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. Se puede aplicar OR a las marcas TCP durante el intervalo de agregación. Para conexiones breves, los marcadores se pueden establecer en la misma línea en el registro de flujo, por ejemplo 19 para SYN-ACK y FIN 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 interfaz donde se captura el tráfico. 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 para el campo 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 para el campo dstaddr campo, si la dirección IP de destino es para un AWS servicio. Para ver una lista de los valores posibles, 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 de los permisos necesarios a los usuarios de IAM para los EC2 recursos de Amazon en la referencia de la EC2 API de Amazon.

A continuación se muestra una política de ejemplo que concede a los usuarios permisos completos para crear, describir y eliminar logs de flujo.

```
{
  "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, en función de si va a publicar en CloudWatch Logs o en Amazon S3. Para obtener más información, consulte Transit Gateway Flow registra registros en Amazon CloudWatch Logs y Entradas de registros de flujo de Transit Gateways 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.

Creación o actualización de un rol de IAM para los registros de flujo de Amazon VPC Transit Gateways

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 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 Next (Siguiente).
5. En la página Nombre, revise y cree página, especifique un nombre para el rol y, opcionalmente, 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.

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.

```
{
  "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.

```
{
  "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.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Cree un registro de registros de flujo de Transit Gateways 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 AWS Management Console 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 AWS default format (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 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 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 Create alarm (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 Next (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).

Entradas de registros de flujo de Transit Gateways 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

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.

```
{
```

```
  "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, consulta las políticas de buckets en la Guía del usuario de Amazon Simple Storage Service.

```
{
    "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:region: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:region: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.

Creación de un rol de la cuenta de origen para los registros de flujo de Transit Gateway 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 AWS Management Console 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 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 Next (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).

Creación de un registro de flujo de Transit Gateway que 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 AWS default format (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/'
```

Consulta de entradas de registros de flujo de 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).

Entradas de registros de flujo procesadas 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.

Entradas de registros de flujo de Transit Gateway en Amazon Data Firehose

Temas

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 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`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region: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::destination-account: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.

```
{
  "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.

```
{
  "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.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Creación del rol de cuenta de origen para los registros de flujo de Transit Gateway para Amazon 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 AWS Management Console 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 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 Next (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).

Creación del rol de cuenta de destino para los registros de flujo de Transit Gateway 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 AWS Management Console 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 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 Next (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).

Creación de una entrada de registro de flujo de Transit Gateway que 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, consulta 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 AWS default format (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 Amazon VPC Transit Gateways mediante APIs la CLI

Puede utilizar la línea de comandos para realizar las tareas descritas en esta página.

Al utilizar el comando, se aplican las siguientes limitaciones: create-flow-logs

- `--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)

Consulta de entradas de registros de flujo de Amazon VPC Transit Gateways

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.

Administración de las etiquetas de los registros de flujo de Amazon VPC Transit Gateways

Puede añadir o eliminar etiquetas de 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.

Búsqueda de entradas de registros de flujo de Amazon VPC Transit Gateways

Puede buscar los registros de registro de flujo que están publicados en CloudWatch Logs mediante la consola de CloudWatch Logs. 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]
```

Eliminación de una entrada de registro de flujo de Amazon VPC Transit Gateways

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 Amazon VPC Transit Gateways

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 Amazon VPC Transit Gateways.

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 registros.

CloudWatch Eventos que utilizan Network Manager

Puede utilizarlos AWS Network Manager para reenviar CloudWatch eventos y luego enrutarlos a funciones o transmisiones de destino. 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 Amazon VPC Transit Gateways

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 métricas de Transit Gateway 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 descartados debido a la caducidad del TTL. Estadísticas: la única estadística relevante es Sum.

Métricas de nivel de adjunto 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 las zonas de disponibilidad están disponibles si están habilitadas para las zonas de disponibilidad de las pasarelas de tránsito adjuntas. AZs Solo los adjuntos de VPC admiten métricas por zona de disponibilidad. Todas las métricas de nivel AZ se publican en la cuenta del propietario de la pasarela de transporte. Las métricas AZ individuales de un adjunto también se publican en la cuenta del propietario del adjunto. El propietario del adjunto solo puede ver las métricas por zona de disponibilidad de su propio adjunto.

Siempre se informan todas las métricas. Sus valores dependen del tráfico que entra o sale de la conexión de puerta de enlace de tránsito. Consulte Dimensiones métricas de Transit Gateway 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`.
`PacketsIn`	El número de paquetes recibidos por la gateway de tránsito desde la conexión.

Métrica	Descripción
	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 descartados debido a la caducidad del TTL. Estadísticas: la única estadística relevante es `Sum`.

Dimensiones métricas de Transit Gateway

Filtre los datos métricos de la pasarela 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.
`TransitGateway` , `AvailabilityZone`	Filtra los datos métricos por pasarela de tránsito y zona de disponibilidad.

Dimensión	Descripción
`TransitGatewayAttachment` , `AvailabilityZone`	Filtra los datos de las métricas por conexión a la pasarela de tránsito y por zona de disponibilidad.

Registro de llamadas a la API de Amazon VPC Transit Gateways con AWS CloudTrail

Amazon VPC Transit Gateways 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 AWS Management Console son multirregionales. Puede crear un registro de seguimiento de una sola región o de varias regiones 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.

Amazon VPC Transit Gateways 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 Amazon VPC Transit Gateways en las que Transit Gateway inicia sesión CloudTrail, consulte la referencia de API de Amazon VPC Transit Gateways.

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"
}
```

Administración de identidades y accesos en Amazon VPC Transit Gateways

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`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCreateTaggedTGWs",
            "Effect": "Allow",
            "Action": "ec2:CreateTransitGateway",
            "Resource": "arn:aws:ec2:region:account-id:transit-gateway/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/stack": "prod"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "stack"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id: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`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteTransitGatewayRouteTable",
                "ec2:CreateTransitGatewayRouteTable"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id: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/*"
        }
    ]
}
```

Uso de roles vinculados a servicios para las puertas de enlace de tránsito en Amazon VPC Transit Gateways

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 Roles vinculados al servicio 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 AWSServiceRoleForVPCTransitGateway para 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 rol AWSServiceRoleForVPCTransitGateway confía en los siguientes servicios para asumir el rol:

- `transitgateway.amazonaws.com`

AWSServiceRoleForVPCTransitGateway usa la política administradaAWSVPCTransitGatewayServiceRolePolicy.

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 Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Creación del rol vinculado a servicios

No es necesario crear manualmente el rol de 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 editar la descripción de AWSServiceRoleForVPCTransitGateway mediante IAM. 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 elimine AWSService RoleFor VPCTransit Gateway.

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 eliminar AWSServiceRoleForVPCTransitGateway, Amazon VPC vuelve a crear el rol si adjuntas una VPC de tu cuenta a una pasarela de tránsito.

AWS políticas gestionadas para pasarelas de tránsito en Amazon VPC Transit Gateways

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 de 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: AWSVPCTransit GatewayServiceRolePolicy

Esta política está asociada al rol 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 actualiza las políticas AWS gestionadas

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

Red ACLs para pasarelas de tránsito en Amazon VPC Transit Gateways

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 “La misma subred para las EC2 instancias y la asociación de pasarelas de tránsito”
- the section called “Diferentes subredes para las EC2 instancias y la asociación de pasarelas de tránsito”

La misma subred para las EC2 instancias y la asociación de pasarelas de tránsito

Considere una configuración en la que tenga EC2 instancias y una asociación de pasarela de tránsito en la misma subred. Se usa la misma ACL de red tanto para el tráfico de las EC2 instancias a la puerta de enlace de tránsito como para el tráfico 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 las EC2 instancias y la asociación de pasarelas de tránsito

Considere una configuración en la que tenga EC2 instancias en una subred y una asociación de puerta de enlace de tránsito en una subred diferente, y cada subred esté asociada a una ACL de red diferente.

Las reglas de ACL de red se aplican de la siguiente manera a la subred de la instancia 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. Para cada subred, usa un CIDR pequeño, por ejemplo /28, de modo que tengas más direcciones para los recursos. 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 aplicarlo NACLs 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”.

Cuotas de Amazon VPC Transit Gateways

Cuenta de AWS Tiene las siguientes cuotas (anteriormente denominadas límites) relacionadas 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

Nombre	Valor 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

Nombre	Valor 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	Sí

Nombre	Valor predeterminado	Ajustable
Rutas dinámicas anunciadas desde un dispositivo de enrutador virtual a una interconexión de Connect	1 000	Sí
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.

Nombre	Valor predeterminado	Ajustable
Conexiones por puerta de enlace de tránsito	5 000	No
Puertas de enlace 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
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

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), la configuración o limitación de las políticas 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 AWS 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.

Nombre	Valor predeterminado	Ajustable
Ancho de banda por adjunto de VPC por zona de disponibilidad	Hasta 100 Gbps	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 administrador técnico de cuentas (TAM) para obtener más ayuda.
Ancho de banda para la conexión de AWS Direct Connect pasarela o pasarela de tránsito interconectada por zona de disponibilidad disponible en la región	Hasta 100 Gbps	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 (AWS Direct Connect	Hasta 7 500 000	Póngase en contacto con su arquitecto de soluciones (SA) o su

Nombre	Valor predeterminado	Ajustable
y adjuntos de interconexión) por zona de disponibilidad disponible en la región		administrador técnico de cuentas (TAM) para obtener más ayuda.
Ancho de banda máximo por túnel de VPN	Hasta 1,25 Gbps	No
Paquetes máximos por segundo por túnel de VPN	Hasta 140 000	No
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 AWS 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.

AWS Direct Connect puertas de enlace

Nombre	Valor predeterminado	Ajustable
AWS Direct Connect pasarelas por pasarela de tránsito	20	No
Pasarelas de tránsito por puerta de enlace AWS 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). AWS 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 pasarelas de tránsito admiten Path MTU Discovery (PMTUD) para el tráfico que ingresa a los archivos adjuntos de VPC y Connect. La pasarela de tránsito genera los paquetes para y `FRAG_NEEDED` para los paquetes ICMPv4 . `Packet Too Big (PTB)` ICMPv6 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 Transit Gateway no sea adecuada para operaciones de alta frecuencia o aplicaciones sensibles al rendimiento. Te recomendamos encarecidamente que revises los siguientes límites de multidifusión. Póngase en contacto con su cuenta o con el equipo de arquitectos de soluciones para obtener una revisión detallada de sus requisitos de rendimiento.

Nombre	Valor predeterminado	Ajustable
Dominios de multidifusión por puerta de enlace de tránsito	20	Sí
Interfaces de red de multidifusión por puerta de enlace de tránsito	10 000	Sí
Asociaciones de dominios de multidifusión por VPC	20	Sí
Fuentes por grupo de multidifusión de puerta de enlace de tránsito	1	Sí
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

Nombre	Valor predeterminado	Ajustable
Cantidad máxima de paquetes por segundo por flujo (menos de 10 receptores)	75 000	No
Cantidad máxima de paquetes 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 red

Nombre	Valor 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 AWS 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
Adjuntos de funciones de red	Cree un accesorio de función de red al que conectar directamente una pasarela de tránsito AWS Network Firewall.	16 de junio de 2025
Compatibilidad de referencia a grupos de seguridad	Ahora puede hacer referencia a un grupo de seguridad VPCs conectado a una pasarela 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	Transit Gateway admite el enrutamiento del tráfico de multidifusión entre subredes conectadas VPCs y sirve como enrutador de 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 AWS Direct Connect puerta de enlace para conectar su AWS Direct Connect conexión a través de una interfaz virtual de tránsito a la puerta de enlace de tránsito VPCs o VPNs conectada a ella.	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.