
Amazon Virtual Private Cloud

Interconexión de VPC



Amazon Virtual Private Cloud: Interconexión de VPC

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

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

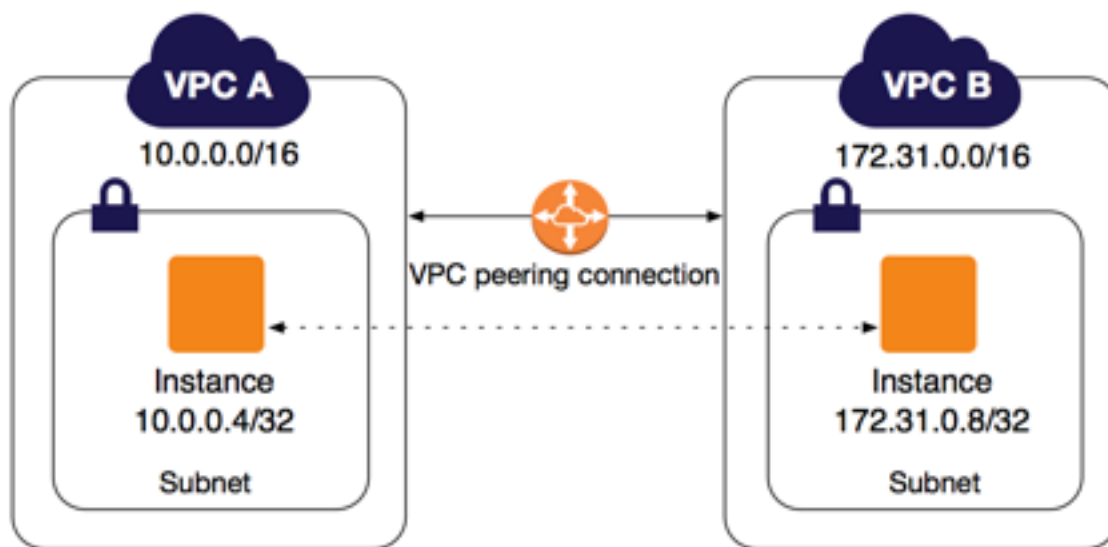
Table of Contents

¿Qué es una interconexión de VPC?	1
Precios de las interconexiones de VPC	2
Conceptos básicos de las interconexiones de VPC	2
Ciclo de vida de las interconexiones de VPC	2
Conexiones de emparejamiento de múltiples VPC	4
Limitaciones de interconexión de VPC	4
Interconexiones de VPC	6
Creación y aceptación	6
Cree una interconexión de VPC con otra VPC de su cuenta	6
Cree una interconexión de VPC con una VPC de otra cuenta de AWS	7
Aceptación de una interconexión de VPC	9
Visualice sus interconexiones de VPC	10
Rechazo	10
Actualización de las tablas de ruteo	10
Referencia a grupos de seguridad de la VPC del mismo nivel	12
Identifique los grupos de seguridad a los que se hace referencia	13
Trabaje con reglas de grupo de seguridad obsoletas	14
Modificación de las opciones de interconexión	15
Habilite la resolución de DNS para la interconexión de VPC	15
Eliminar	16
Escenarios de interconexión de VPC	18
Interconexión de dos o más VPC para proporcionar acceso completo a los recursos	18
Interconexión de una VPC para obtener acceso a recursos centralizados	18
Interconexión con ClassicLink	19
Configuraciones de interconexión de VPC	20
Configuraciones con rutas a un bloque de CIDR completo	20
Utilización de dos VPC interconectadas	20
Una VPC interconectada a dos VPC	22
Tres VPC interconectadas	25
Una VPC interconectada a varias VPC	27
Varias VPC interconectadas	31
Configuraciones con rutas específicas	39
Dos VPC interconectadas a dos subredes de una VPC	40
Dos VPC interconectadas a dos bloques de CIDR diferentes en una VPC	44
Una VPC interconectada a subredes específicas de dos VPC	45
Instancias de una VPC interconectada a instancias de dos VPC	48
Una VPC interconectada a dos VPC mediante la coincidencia con el prefijo de mayor longitud	50
Múltiples configuraciones de VPC	51
Configuraciones con ClassicLink	53
Habilitación de la comunicación entre una instancia ClassicLink y una VPC del mismo nivel	55
Configuraciones de interconexión de VPC no admitidas	61
Bloques de CIDR solapados	61
Interconexión transitiva	62
Enrutamiento de borde a borde mediante una gateway o una conexión privada	62
Identity and Access Management	65
Creación de una interconexión de VPC	65
Aceptación de una interconexión de VPC	66
Eliminación de una interconexión de VPC	67
Funcionamiento de una cuenta específica	67
Administración de las interconexiones de VPC en la consola	68
Historial de revisión	69

¿Qué es una interconexión de VPC?

[Amazon Virtual Private Cloud](#) (Amazon VPC) le permite lanzar recursos de AWS en una red virtual que haya definido.

Una interconexión de VPC es una conexión de redes entre dos VPC que permite direccionar tráfico entre ellas mediante direcciones IPv6 o direcciones IPv4 privadas. Las instancias de ambas VPC se pueden comunicar entre sí siempre que se encuentren en la misma red. Puede crear una interconexión de VPC entre sus propias VPC o con una VPC de otra cuenta de AWS. Las VPC pueden encontrarse en regiones distintas (lo que se conoce como interconexión de VPC entre regiones).



AWS utiliza la infraestructura existente de una VPC para crear una interconexión de VPC. No se trata de ninguna gateway o conexión de VPN y no usa ningún hardware físico individual. Por lo tanto, no existen puntos de error de comunicaciones ni cuellos de botella de ancho de banda.

Una interconexión de VPC le ayuda a facilitar la transferencia de datos. Por ejemplo, si tiene más de una cuenta de AWS, puede interconectar las VPC de dichas cuentas para crear una red de uso compartido de archivos. También puede utilizar la interconexión de VPC para que otras VPC puedan obtener acceso a los recursos que tiene en una de sus VPC.

Puede establecer relaciones de interconexión entre VPC en diferentes regiones de AWS (también denominado emparejamiento de VPC entre regiones). Esto permite que los recursos de VPC como las instancias EC2, las bases de datos de Amazon RDS y las funciones de Lambda que se ejecutan en distintas regiones de AWS se comuniquen entre sí utilizando direcciones IP privadas, sin necesidad de usar gateways, conexiones VPN ni dispositivos de red independientes. El tráfico permanece en el espacio de direcciones IP privadas. Todo el tráfico entre regiones está cifrado y no tiene un punto de error único ni un cuello de botella en el ancho de banda. El tráfico siempre permanece en la red troncal global de AWS y nunca pasa por la red pública de Internet, lo que reduce los vectores de amenazas, como las vulnerabilidades comunes y los ataques DDoS. La interconexión de VPC entre regiones proporciona una forma sencilla y rentable de compartir recursos entre regiones o de replicar datos para obtener redundancia geográfica.

Precios de las interconexiones de VPC

No se aplica ningún cargo por crear un emparejamiento de VPC. Hay un cargo por la transferencia de datos a través de conexiones de intercambio de tráfico. Para obtener más información, consulte [Precios de Amazon EC2](#).

Conceptos básicos de las interconexiones de VPC

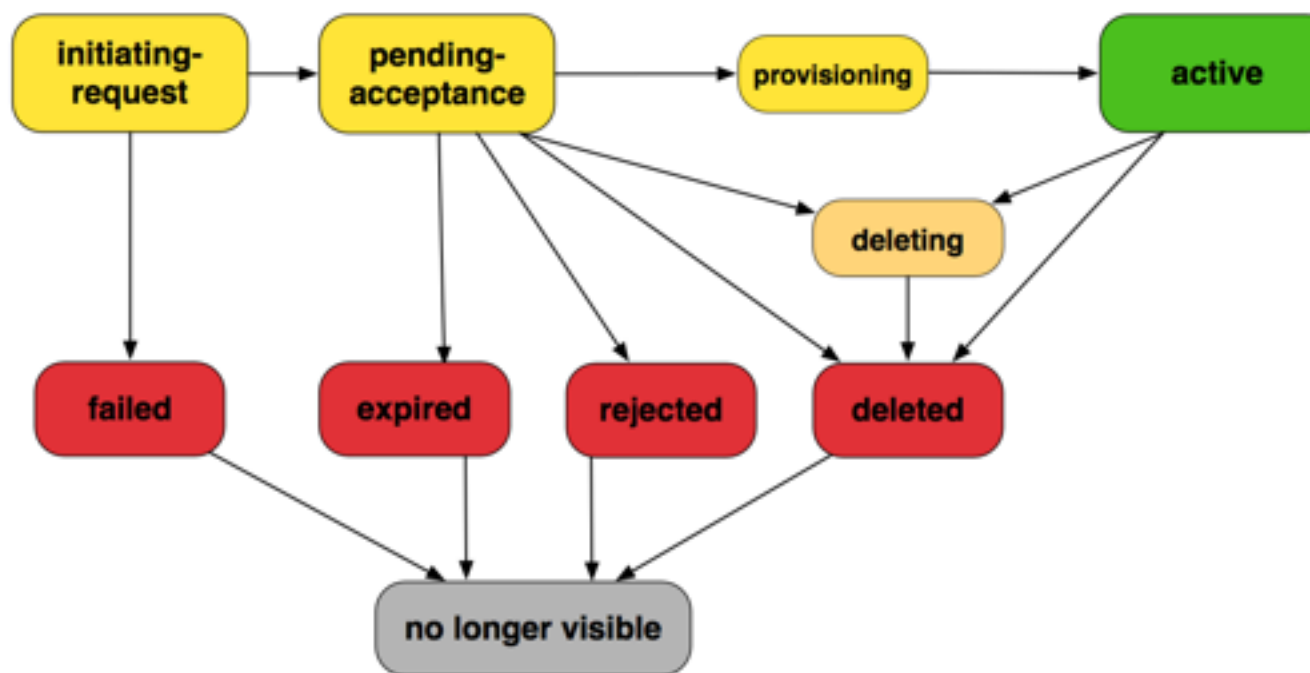
Para establecer una interconexión de VPC, realice lo siguiente:

1. El propietario de la VPC solicitante envía una solicitud al propietario de la VPC que acepta la solicitud para crear la interconexión de VPC. La VPC del que acepta puede ser de su propiedad o de otra cuenta de AWS, y no puede tener un bloque de CIDR que se superponga con el bloque de CIDR de la VPC del solicitante.
2. El propietario de la VPC responsable de la aceptación debe aceptar la solicitud de interconexión de VPC para activar la interconexión de VPC.
3. Para permitir el flujo de tráfico entre VPC mediante direcciones IP privadas, los propietarios de las VPC de la interconexión deben añadir manualmente una ruta a una o varias de las tablas de ruteo de sus VPC que apunten al rango de direcciones IP de la otra VPC (VPC del mismo nivel).
4. Si es necesario, actualice las reglas del grupo de seguridad asociadas a su instancia para asegurarse de que el tráfico entrante y saliente de la VPC del mismo nivel no se vea afectado. Si ambas VPC se encuentran en la misma región, puede hacer referencia a un grupo de seguridad desde la VPC del mismo nivel como origen o destino de reglas de tráfico entrante o saliente del grupo de seguridad.
5. Con las opciones predeterminadas de interconexión de VPC, si las instancias EC2 de ambos extremos de una interconexión de VPC direccionan el tráfico entre sí utilizando un nombre de host DNS público, el nombre de host se resuelve en la dirección IP pública de la instancia. Para cambiar este comportamiento, habilite la resolución de nombres del host DNS para su conexión de VPC. Después de habilitar la resolución de nombres del host de DNS, si las instancias de ambos extremos de la interconexión de VPC se comunican entre sí utilizando un nombre de host DNS público, el nombre de host se resuelve en la dirección IP privada de la instancia.

Para obtener más información, consulte [Trabaje con interconexiones de VPC \(p. 6\)](#).

Ciclo de vida de las interconexiones de VPC

Las interconexiones de VPC pasan 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 interconexión de VPC permanecerá visible en la consola de Amazon VPC y en la API o los resultados de la línea de comandos durante un periodo de tiempo.



- **Initiating-request:** se ha iniciado una solicitud de interconexión de VPC. En esta fase, es posible que se produzca un error en la interconexión o puede ir a **pending-acceptance**.
- **Failed:** se ha producido un error en la solicitud de interconexión de VPC. Mientras esté en este estado, no se puede aceptar, rechazar o eliminar. La interconexión de VPC con error permanecerá visible al solicitante durante 2 horas.
- **Pending-acceptance:** la solicitud de interconexión de VPC está pendiente de la aceptación del propietario de la VPC responsable de aceptar la solicitud. Con este estado, el propietario de la VPC solicitante podrá eliminar la solicitud. Por su parte, el propietario de la otra VPC podrá aceptar o rechazar la solicitud. Si no se realiza ninguna acción, la solicitud caducará transcurridos 7 días.
- **Expired:** la solicitud de interconexión de VPC ha caducado. Con este estado, los propietarios de las VPC no podrán realizar ninguna acción. La interconexión de VPC caducada permanecerá visible para ambos propietarios de VPC durante 2 horas.
- **Rejected:** el propietario de la VPC responsable de aceptar la solicitud ha rechazado la solicitud de interconexión de VPC con el estado **pending-acceptance**. Mientras esté en este estado, no se puede aceptar la solicitud. La interconexión de VPC rechazada permanecerá visible para el propietario de la VPC solicitante durante 2 días y durante 2 horas para el propietario de la VPC responsable de aceptar la solicitud. Si la solicitud se creó desde la misma cuenta de AWS, la solicitud rechazada permanecerá visible durante 2 horas.
- **Provisioning:** la solicitud de interconexión de VPC se ha aceptado y pronto pasará al estado **active**.
- **Active:** la interconexión de VPC está activa y el tráfico puede fluir entre las VPC (siempre que los grupos de seguridad y las tablas de ruteo lo permitan). Mientras se encuentre en este estado, cualquiera de los propietarios de la VPC puede eliminar la interconexión de VPC, pero no puede rechazarla.

Note

Si ocurre un evento en una región en la que reside una VPC impide el flujo del tráfico, el estado de la interconexión de VPC continúa siendo **Active**.

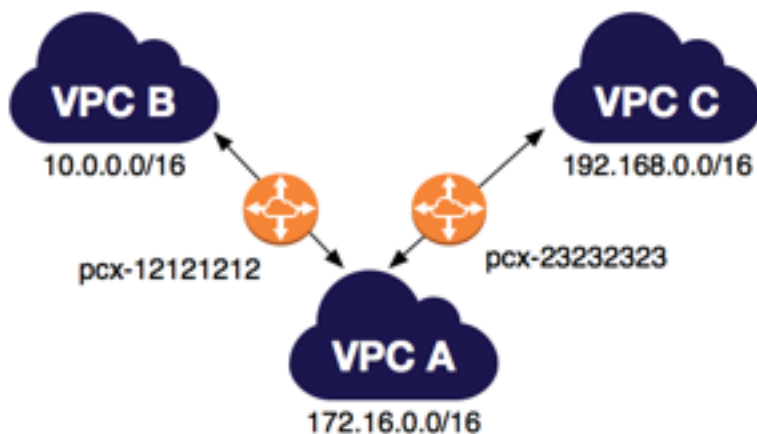
- **Deleting:** se refiere a una interconexión de VPC en regiones distintas que se encuentra en proceso de eliminación. El propietario de una de las VPC ha enviado una solicitud para eliminar una interconexión de VPC en estado **active**, o bien el propietario de la VPC solicitante ha enviado una petición para eliminar una solicitud de interconexión de VPC en estado **pending-acceptance**.

- Deleted: un propietario de una de las VPC ha eliminado una interconexión de VPC con el estado `active`, o bien el propietario de la VPC solicitante ha eliminado la solicitud de interconexión de VPC que tenía el estado `pending-acceptance`. Mientras se encuentre en este estado, no se puede aceptar ni rechazar la interconexión de VPC. La interconexión de VPC permanecerá visible para la parte que la eliminó durante 2 horas y durante 2 días para la otra parte. Si la interconexión de VPC se creó desde la misma cuenta de AWS, la solicitud eliminada permanecerá visible durante 2 horas.

Conexiones de emparejamiento de múltiples VPC

Una interconexión de VPC es una relación de uno a uno entre dos VPC. Puede crear conexiones de emparejamiento de múltiples VPC para cada VPC que posea, pero las relaciones de emparejamiento transitivo no están admitidas. No podrá crear relaciones de interconexión con VPC a las que su VPC no esté interconectada directamente.

El diagrama siguiente muestra un ejemplo de una VPC interconectada a varias VPC. Existen dos interconexiones de VPC: la VPC A está interconectada con la VPC B y la VPC C. La VPC B y la VPC C no están interconectadas, por lo que no puede utilizar la VPC A como punto de tránsito para interconectar la VPC B y la VPC C. Si desea habilitar el direccionamiento de tráfico entre la VPC B y la VPC C, debe crear una interconexión de VPC única entre estas VPC.



Limitaciones de interconexión de VPC

Para crear una interconexión de VPC con otra VPC, tenga en cuenta las siguientes reglas y limitaciones:

- No puede crear una interconexión de VPC entre VPC con los mismos bloques de CIDR IPv4 o IPv6 o con bloques solapados. Amazon siempre asigna a su VPC un bloque de CIDR IPv6 único. Si sus bloques de CIDR IPv6 son únicos pero los bloques de IPv4 no lo son, no podrá crear la interconexión.
- Hay una cuota establecida en el número de interconexiones de VPC activas y pendientes que puede tener por cada VPC. Para obtener más información, consulte [Cuotas de Amazon VPC](#) en la Guía del usuario de Amazon VPC.
- La interconexión de VPC no admite relaciones de interconexión transitivas. En una interconexión de VPC, su VPC no tiene acceso a otras VPC que puedan estar interconectadas con la VPC del mismo nivel. Esto incluye las interconexiones de VPC establecidas en su totalidad en su propia cuenta de AWS. Para obtener más información acerca de las relaciones de interconexión no compatibles, consulte [Configuraciones de interconexión de VPC no admitidas](#) (p. 61). Para obtener ejemplos de relaciones de interconexión compatibles, consulte [Escenarios de interconexión de VPC](#) (p. 18).
- No puede tener más de una interconexión de VPC entre las mismas VPC a la vez.

- No se admite el reenvío de rutas inversas unidifusión en interconexiones de VPC. Para obtener más información, consulte [Enrutamiento del tráfico de respuesta \(p. 46\)](#).
- Es posible habilitar la comunicación entre los recursos de ambos extremos de una interconexión de VPC mediante IPv6; sin embargo, la comunicación mediante IPv6 no es automática. Deberá asociar un bloque de CIDR IPv6 a cada VPC, habilitar la comunicación mediante IPv6 en las instancias de las VPC y añadir rutas a las tablas de ruteo para direccionar el tráfico IPv6 con destino a la VPC del mismo nivel a la interconexión de VPC. Para obtener más información, consulte [VPC y subredes](#) en la Guía del usuario de Amazon VPC.
- Las etiquetas que cree para la interconexión VPC solo se aplicarán en la cuenta o región en las que las haya creado.
- Si el bloque de CIDR de IPv4 de una VPC en una interconexión de VPC queda fuera de los rangos de direcciones IPv4 privadas especificado por [RFC 1918](#), los nombres de host de DNS privada para dicha VPC no se pueden resolver en direcciones IP privadas. Para resolver los nombres de host de DNS privada a direcciones IP privadas, puede habilitar la compatibilidad de resolución DNS para la interconexión de VPC. Para obtener más información, consulte [Habilite la resolución de DNS para la interconexión de VPC \(p. 15\)](#).
- No puede conectarse ni consultar el servidor DNS de Amazon en una VPC del mismo nivel.

Una interconexión de VPC entre regiones tiene limitaciones adicionales:

- No es posible crear una regla grupo de seguridad referida a un grupo de seguridad de una VPC interconectada.
- No es posible habilitar el uso de una instancia de EC2-Classik vinculada a una VPC mediante ClassicLink para comunicarse con la VPC interconectada,
- La unidad de transmisión máxima (MTU) a través de la interconexión de VPC es 1500 bytes (no se admiten tramas gigantes).
- Debe habilitar la compatibilidad con la resolución de DNS para que la interconexión de VPC resuelva los nombres de host DNS privados de la VPC del mismo nivel en direcciones IP privadas, incluso si el CIDR IPv4 de la VPC está incluido en los intervalos de direcciones IPv4 privadas especificados por RFC 1918.

Trabaje con interconexiones de VPC

Puede utilizar la consola de Amazon VPC para crear y trabajar con interconexiones de VPC.

Tareas

- [Cree y acepte las interconexiones de VPC](#). (p. 6)
- [Rechace la interconexión de VPC](#) (p. 10)
- [Actualice sus tablas de enrutamiento para interconexiones de VPC](#) (p. 10)
- [Actualice sus grupos de seguridad para que hagan referencia a grupos de la VPC del mismo nivel](#) (p. 12)
- [Modifique las opciones de interconexión de VPC](#) (p. 15)
- [Elimine la interconexión de VPC](#) (p. 16)

Cree y acepte las interconexiones de VPC.

Para crear una interconexión de VPC, primero debe crear una solicitud de emparejamiento con otra VPC. Puede solicitar una interconexión de VPC con otra VPC de su cuenta o con una VPC de otra cuenta de AWS distinta. Si en una interconexión de VPC las VPC se encuentran en regiones distintas, la solicitud debe provenir de la región de la VPC solicitante.

Para activar la solicitud, el propietario de la VPC debe aceptar la solicitud. Para que se produzca la interconexión de VPC en regiones distintas, la solicitud debe aceptarse en la región de la VPC receptora.

Antes de empezar, asegúrese de que conoce las [limitaciones y reglas](#) (p. 4) de una interconexión de VPC.

Tareas

- [Cree una interconexión de VPC con otra VPC de su cuenta](#) (p. 6)
- [Cree una interconexión de VPC con una VPC de otra cuenta de AWS](#) (p. 7)
- [Aceptación de una interconexión de VPC](#) (p. 9)
- [Visualice sus interconexiones de VPC](#) (p. 10)

Cree una interconexión de VPC con otra VPC de su cuenta

Para solicitar una interconexión de VPC con una VPC de su cuenta, asegúrese de que dispone de los ID de las VPC para las que va a crear la interconexión de VPC. Deberá crear y aceptar la solicitud de interconexión de VPC para activarla.

Puede crear una interconexión de VPC con una VPC de la misma región o de una región distinta.

Important

Asegúrese de que su VPC no tenga bloques de CIDR IPv4 que se solapen. En caso contrario, el estado de la interconexión de VPC cambiará inmediatamente a `failed`. Esta limitación se aplica incluso cuando las VPC tengan bloques de CIDR IPv6.

Para crear una interconexión de VPC con una VPC de la misma región, haga lo siguiente:

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections, Create Peering Connection.
3. Configure la información siguiente y elija Create Peering Connection cuando haya terminado:

- Peering connection name tag: de manera opcional, puede asignar un nombre a su interconexión de VPC.
- VPC (Requester): seleccione la VPC de su cuenta con la que desea crear la interconexión de VPC.
- En Select another VPC to peer with: compruebe que está seleccionado My account y seleccione otra de sus VPC.
- Como opción, agregue o elimine una etiqueta.

[Añadir una etiqueta] Elija Add tag (Añadir etiqueta) y haga lo siguiente:

- En Key (Clave), escriba el nombre de la clave.
- En Value (Valor), escriba el valor de la clave.

[Eliminar una etiqueta] Elija el botón Eliminar ("X") situado a la derecha de la clave y valor de la etiqueta.

4. En el cuadro de diálogo de confirmación, elija OK.
5. Seleccione la interconexión de VPC que ha creado y elija Actions, Accept Request.
6. En el cuadro de diálogo de confirmación, elija Yes, Accept. Aparecerá un segundo cuadro de diálogo de confirmación. Elija Modify my route tables now para ir directamente a la página de las tablas de ruteo, o bien elija Close para realizar esta acción más adelante.

Para crear una interconexión de VPC con una VPC de una región diferente, haga lo siguiente:

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections, Create Peering Connection.
3. Configure la información siguiente y elija Create Peering Connection cuando haya terminado:
 - Peering connection name tag: de manera opcional, puede asignar un nombre a su interconexión de VPC. Esta acción creará una etiqueta con una clave de Name y el valor que especifique.
 - VPC (Requester): seleccione la VPC solicitante en su cuenta con la que solicitará la interconexión de VPC.
 - Account: compruebe que está seleccionado My account.
 - Region (Región): elija Another region (Otra región) y seleccione la región en la que reside la VPC receptora.
 - VPC (Acceptor): Escriba el ID de la VPC receptora.
4. En el cuadro de diálogo de confirmación, elija OK.
5. En el selector de regiones, seleccione la región de la VPC receptora.
6. En el panel de navegación, elija Peering Connections. Seleccione la interconexión de VPC que ha creado y elija Actions, Accept Request.
7. En el cuadro de diálogo de confirmación, elija Yes, Accept. Aparecerá un segundo cuadro de diálogo de confirmación. Elija Modify my route tables now para ir directamente a la página de las tablas de ruteo, o bien elija Close para realizar esta acción más adelante.

Ahora que su interconexión de VPC está activa, deberá añadir una entrada en las tablas de ruteo de la VPC para permitir el direccionamiento del tráfico entre las VPC interconectadas. Para obtener más información, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Cree una interconexión de VPC con una VPC de otra cuenta de AWS

Puede solicitar una interconexión de VPC con una VPC de otra cuenta de AWS. Antes de comenzar, asegúrese de que dispone del número de cuenta de AWS y del ID de VPC de la VPC con la que desea

crear la interconexión. Tras crear la solicitud, el propietario de la VPC que acepte la interconexión deberá aceptar la interconexión de VPC para activarla.

Puede crear una interconexión de VPC con una VPC de la misma región o de una región distinta.

Important

Si las VPC tienen bloques de CIDR IPv4 solapados, o si el ID de cuenta o el ID de VPC son incorrectos o no se corresponden entre sí, el estado de la interconexión de VPC cambiará inmediatamente a `failed`.

Para solicitar una interconexión de VPC con una VPC de otra cuenta de la misma región, haga lo siguiente:

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections, Create Peering Connection.
3. Configure la información como se indica a continuación y elija Create Peering Connection cuando haya terminado:
 - Peering connection name tag: de manera opcional, puede asignar un nombre a su interconexión de VPC. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique. Esta etiqueta solo está visible para usted. El propietario de la VPC del mismo nivel puede crear sus propias etiquetas para la interconexión de VPC.
 - VPC (Requester): seleccione la VPC de su cuenta con la que va a crear la interconexión de VPC.
 - Account: elija Another account.
 - Account ID (ID de la cuenta): ingrese el ID de la cuenta de AWS del propietario de la VPC receptora.
 - VPC (Accepter): escriba el ID de la VPC de su cuenta con la que va a crear la interconexión de VPC.
4. En el cuadro de diálogo de confirmación, elija OK.

Para solicitar una interconexión de VPC con una VPC de otra cuenta de una región distinta, haga lo siguiente:

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections, Create Peering Connection.
3. Configure la información como se indica a continuación y elija Create Peering Connection cuando haya terminado:
 - Peering connection name tag: de manera opcional, puede asignar un nombre a su interconexión de VPC. Esta acción creará una etiqueta con una clave de `Name` y el valor que especifique. Esta etiqueta solo está visible para usted. El propietario de la VPC del mismo nivel puede crear sus propias etiquetas para la interconexión de VPC.
 - VPC (Requester): seleccione la VPC de su cuenta con la que va a crear la interconexión de VPC.
 - Account: elija Another account.
 - Account ID (ID de la cuenta): ingrese el ID de la cuenta de AWS del propietario de la VPC receptora.
 - Region (Región): elija Another region (Otra región) y seleccione la región en la que reside la VPC receptora.
 - VPC (Accepter): escriba el ID de la VPC de su cuenta con la que va a crear la interconexión de VPC.
4. En el cuadro de diálogo de confirmación, elija OK.

La interconexión de VPC que ha creado no está activa. Para activarla, el propietario de la VPC que acepte la interconexión deberá aceptar la solicitud de interconexión de VPC. Actualice la tabla de ruteo de su

VPC para permitir el direccionamiento de tráfico a la VPC del mismo nivel. Para obtener más información, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Para crear una interconexión de VPC mediante la línea de comandos o una API

- [create-vpc-peering-connection](#) (AWS CLI)
- [New-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [CreateVpcPeeringConnection](#) (API de consulta de Amazon EC2)

Aceptación de una interconexión de VPC

El propietario de la VPC que acepte la interconexión debe aceptar las interconexiones de VPC con el estado `pending-acceptance` para que puedan activarse. No puede aceptar solicitudes de interconexiones de VPC que haya enviado a otra cuenta de AWS. Si va a crear una interconexión de VPC en la misma cuenta de AWS, deberá crear y aceptar la solicitud usted mismo.

Si las VPC se encuentran en regiones distintas, la solicitud debe aceptarse en la región de la VPC receptora.

Important

No acepte interconexiones de VPC de cuentas de AWS que no conozca, ya que los usuarios malintencionados pueden enviar solicitudes de interconexión de VPC para obtener acceso no autorizado a su VPC. Esto se denomina ataques de phishing de interconexión. De este modo, puede rechazar con seguridad las solicitudes de interconexión de VPC sin correr el riesgo de que el solicitante obtenga acceso a información acerca de su cuenta de AWS o su VPC. Para obtener más información, consulte [Rechace la interconexión de VPC \(p. 10\)](#). También puede omitir estas solicitudes y dejar que caduquen. De manera predeterminada, las solicitudes a los 7 días.

Para aceptar una interconexión de VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el selector de regiones, seleccione la región de la VPC receptora.
3. En el panel de navegación, elija Peering Connections.
4. Seleccione la interconexión de VPC pendiente (con el estado `pending-acceptance`) y elija Actions, Accept Request.

Note

Si no ve la interconexión de VPC pendiente, compruebe la región. La solicitud de interconexión entre regiones distintas debe aceptarse en la región de la VPC receptora.

5. En el cuadro de diálogo de confirmación, elija Yes, Accept. Aparecerá un segundo cuadro de diálogo de confirmación. Elija Modify my route tables now para ir directamente a la página de las tablas de ruteo, o bien elija Close para realizar esta acción más adelante.

Ahora que su interconexión de VPC está activa, deberá añadir una entrada en la tabla de ruteo de su VPC para permitir el direccionamiento del tráfico a la VPC del mismo nivel. Para obtener más información, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Para aceptar una interconexión de VPC mediante la línea de comandos o una API

- [accept-vpc-peering-connection](#) (AWS CLI)
- [Approve-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [AcceptVpcPeeringConnection](#) (API de consulta de Amazon EC2)

Visualice sus interconexiones de VPC

Puede consultar todas las interconexiones de VPC en la consola de Amazon VPC. De forma predeterminada, la consola muestra todas las interconexiones de VPC en los distintos estados, incluidas aquellas que se hayan eliminado o rechazado recientemente. Para obtener más información acerca del ciclo de vida de una interconexión de VPC, consulte [Ciclo de vida de las interconexiones de VPC \(p. 2\)](#).

Para visualizar sus interconexiones de VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections.
3. Aparecerán todas sus interconexiones de VPC. Utilice la barra de búsqueda de filtro para restringir los resultados.

Para describir una interconexión de VPC mediante la línea de comandos o una API

- [describe-vpc-peering-connections](#) (AWS CLI)
- [Get-EC2VpcPeeringConnections](#) (AWS Tools for Windows PowerShell)
- [DescribeVpcPeeringConnections](#) (API de consulta de Amazon EC2)

Rechace la interconexión de VPC

Puede rechazar cualquier solicitud de interconexión de VPC recibida con el estado `pending-acceptance`. Acepte solo interconexiones de VPC de cuentas de AWS que conozca y de su confianza. Rechace aquellas solicitudes no deseadas.

Para rechazar una interconexión de VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections.
3. Seleccione la interconexión de VPC y elija Actions, Reject Request.
4. En el cuadro de diálogo de confirmación, elija Yes, Reject.

Para rechazar una interconexión de VPC mediante la línea de comandos o una API

- [reject-vpc-peering-connection](#) (AWS CLI)
- [Deny-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [RejectVpcPeeringConnection](#) (API de consulta de Amazon EC2)

Actualice sus tablas de enrutamiento para interconexiones de VPC

Para enviar el tráfico IPv4 privado desde su instancia a una instancia de una VPC del mismo nivel, debe añadir una ruta a la tabla de ruteo asociada a su subred en la que reside su instancia. La ruta apunta al bloque de CIDR (o parte del bloque de CIDR) de la VPC del mismo nivel en la interconexión de VPC y especifica la interconexión de VPC como el objetivo.

Del mismo modo, si las VPC de la interconexión de VPC tienen asociados bloques de CIDR IPv6, podrá añadir una ruta a su tabla de ruteo para permitir la comunicación con la VPC del mismo nivel a través de IPv6.

Si una subred no está explícitamente asociada a una tabla de ruteo, esta utilizará la tabla de ruteo principal de forma predeterminada. Para obtener más información, consulte [Tablas de enrutamiento](#) en la Guía del usuario de Amazon VPC.

Tiene una [cuota](#) en el número de entradas que puede agregar por cada tabla de enrutamiento. Si el número de interconexiones de VPC de su VPC supera la cuota de entrada de la tabla de ruteo para una única tabla de ruteo, considere la posibilidad de utilizar varias subredes asociadas a una tabla de ruteo personalizada.

Para obtener más información acerca de las configuraciones de tabla de ruteo compatibles para las interconexiones de VPC, consulte [Configuraciones de interconexión de VPC \(p. 20\)](#).

Puede añadir una ruta para una interconexión de VPC que tenga el estado `pending-acceptance`. Sin embargo, la ruta tendrá el estado de `blackhole` y no tendrá efecto alguno hasta que la interconexión de VPC tenga el estado `active`.

Warning

Si tiene una VPC interconectada con varias VPC con bloques de CIDR IPv4 solapados o que coinciden, asegúrese de que las tablas de ruteo estén configuradas para evitar el envío de tráfico de respuesta desde la VPC a una VPC incorrecta. Actualmente AWS no admite el reenvío de rutas inversas unidifusión en interconexiones de VPC que comprueben la IP de origen de los paquetes y direccionará los paquetes de respuesta de vuelta al origen. Para obtener más información, consulte [Enrutamiento del tráfico de respuesta \(p. 46\)](#).

Para añadir una ruta IPv4 para una interconexión 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.
3. Seleccione la casilla de verificación al lado de la tabla de enrutamiento asociada a la subred en la que reside su instancia.

Note

Si no tiene ninguna tabla de ruteo asociada a dicha subred, seleccione la tabla de ruteo principal de la VPC, ya que la subred utilizará dicha tabla de ruteo de manera predeterminada.

4. Elija Actions (Acciones), Edit routes (Editar rutas).
5. Seleccione Add route (Añadir ruta).
6. En Destination, escriba el rango de direcciones IPv4 al que debe dirigirse el tráfico de red de la interconexión de VPC. Puede especificar el bloque de CIDR IPv4 completo de la VPC del mismo nivel, un rango específico o una dirección IPv4 individual como, por ejemplo, la dirección IP de la instancia con la que desea comunicarse. Por ejemplo, si el bloque de CIDR de la VPC del mismo nivel es `10.0.0.0/16`, puede especificar una porción `10.0.0.0/24` o una dirección IP específica `10.0.0.7/32`.
7. En Target (Destino), seleccione la interconexión de VPC y, a continuación, elija Save changes (Guardar cambios).

El propietario de la VPC del mismo nivel también debe completar estos pasos para agregar una ruta para dirigir el tráfico de vuelta a la VPC a través de la conexión de pares de VPC.

Si tiene recursos en diferentes regiones de AWS en los que se utilizan direcciones IPv6, puede crear una interconexión entre regiones. Luego, puede agregar una ruta IPv6 para la comunicación entre los recursos.

Para añadir una ruta IPv6 para una interconexión 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.

3. Seleccione la casilla de verificación al lado de la tabla de enrutamiento asociada a la subred en la que reside su instancia.

Note

Si no tiene ninguna tabla de ruteo asociada a dicha subred, seleccione la tabla de ruteo principal de la VPC, ya que la subred utilizará dicha tabla de ruteo de manera predeterminada.

4. Elija Actions (Acciones), Edit routes (Editar rutas).
5. Seleccione Add route (Añadir ruta).
6. En Destination, escriba el rango de direcciones IPv6 para la VPC del mismo nivel. Puede especificar el bloque de CIDR IPv6 completo de la VPC del mismo nivel, un rango específico o una dirección IPv6 individual. Por ejemplo, si el bloque de CIDR de la VPC del mismo nivel es `2001:db8:1234:1a00::/56`, puede especificar una porción `2001:db8:1234:1a00::/64` o una dirección IP específica `2001:db8:1234:1a00::123/128`.
7. En Target (Destino), seleccione la interconexión de VPC y, a continuación, elija Save changes (Guardar cambios).

Para obtener más información, consulte [Tablas de enrutamiento](#) en la Guía del usuario de Amazon VPC.

Para añadir o sustituir una ruta mediante la línea de comandos o una API

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (AWS Tools for Windows PowerShell)
- [CreateRoute](#) (API de consulta de Amazon EC2)
- [replace-route](#) (AWS CLI)
- [Set-EC2Route](#) (AWS Tools for Windows PowerShell)
- [ReplaceRoute](#) (API de consulta de Amazon EC2)

Actualice sus grupos de seguridad para que hagan referencia a grupos de la VPC del mismo nivel

Puede actualizar las reglas entrantes o salientes de los grupos de seguridad de su VPC para que hagan referencia a grupos de seguridad de la VPC del mismo nivel. De este modo, garantizará el tráfico entrante y saliente de las instancias asociadas al grupo de seguridad al que se hace referencia en la VPC del mismo nivel.

Requirements

- La VPC del mismo nivel puede ser una VPC de su cuenta o una VPC de otra cuenta de AWS. Para hacer referencia a un grupo de seguridad de otra cuenta de AWS, incluya el número de cuenta en el campo Source (Origen) o Destination (Destino) como, por ejemplo, `123456789012/sg-1a2b3c4d`.
- No es posible hacer referencia al grupo de seguridad de una VPC interconectada que se encuentra en una región distinta. En lugar de ello, utilice el bloque de CIDR de la VPC del mismo nivel.
- Para hacer referencia a un grupo de seguridad de una VPC del mismo nivel, la interconexión de VPC debe tener el estado `active`.
- Si configura rutas para reenviar el tráfico entre dos instancias en subredes diferentes a través de un dispositivo de middlebox, debe asegurarse de que los grupos de seguridad de ambas instancias permiten que el tráfico fluya entre las instancias. El grupo de seguridad de cada instancia debe hacer referencia a la dirección IP privada de la otra instancia, o al rango CIDR de la subred que contiene la otra instancia, como fuente. Si hace referencia al grupo de seguridad de la otra instancia como fuente, esto no permite que el tráfico fluya entre las instancias.

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. Seleccione el grupo de seguridad y elija Inbound Rules (Reglas de entrada) para actualizar las reglas entrantes u Outbound Rules (Reglas de salida) para modificar las reglas salientes.
4. Elija Edit, Add another rule.
5. Especifique el tipo, el protocolo y el rango de puertos según sea necesario. En Source (Origen) (o Destination (Destino) para una regla de salida), escriba el ID del grupo de seguridad de la VPC interconectada si está en la misma región, o el bloque de CIDR de la VPC interconectada si está en una región diferente.

Note

Los grupos de seguridad de una VPC del mismo nivel no se muestran automáticamente.

6. Seleccione Save.

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)

Para actualizar las reglas de salida mediante la línea de comandos

- [authorize-security-group-egress](#) (AWS CLI)
- [Grant-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)
- [Revoke-EC2SecurityGroupEgress](#) (AWS Tools for Windows PowerShell)
- [revoke-security-group-egress](#) (AWS CLI)

Por ejemplo, para actualizar el grupo de seguridad `sg-aaaa1111` para permitir el acceso entrante a través de HTTP desde el grupo `sg-bbbb2222` que se encuentra en una VPC del mismo nivel, puede utilizar el comando de AWS CLI siguiente:

```
aws ec2 authorize-security-group-ingress --group-id sg-aaaa1111 --protocol tcp --port 80 --source-group sg-bbbb2222
```

Una vez actualizadas las reglas del grupo de seguridad, utilice el comando [describe-security-groups](#) para consultar el grupo de seguridad al que se hace referencia en las reglas del grupo de seguridad.

Identifique los grupos de seguridad a los que se hace referencia

Para determinar si se hace referencia a su grupo de seguridad en las reglas de un grupo de seguridad de una VPC del mismo nivel, utilice uno de los comandos siguientes para uno o varios grupos de seguridad de su cuenta.

- [describe-security-group-references](#) (AWS CLI)
- [Get-EC2SecurityGroupReference](#) (AWS Tools for Windows PowerShell)
- [DescribeSecurityGroupReferences](#) (API de consulta de Amazon EC2)

En el siguiente ejemplo, la respuesta indica que un grupo de seguridad de la VPC `sg-bbbb2222` hace referencia al grupo de seguridad `vpc-aaaaaaa`:

```
aws ec2 describe-security-group-references --group-id sg-bbbb2222
```

```
{
  "SecurityGroupsReferenceSet": [
    {
      "ReferencingVpcId": "vpc-aaaaaaa",
      "GroupId": "sg-bbbb2222",
      "VpcPeeringConnectionId": "pcx-b04deed9"
    }
  ]
}
```

Si se elimina la interconexión de VPC o si el propietario de la VPC del mismo nivel elimina el grupo de seguridad al que se hace referencia, la regla del grupo de seguridad quedará obsoleta.

Trabaje con reglas de grupo de seguridad obsoletas

Las reglas de grupos de seguridad obsoletas son aquellas que hacen referencia a un grupo de seguridad eliminado en la misma VPC o en una VPC del mismo nivel, o que hace referencia a un grupo de seguridad en una VPC del mismo nivel para la que se ha eliminado la conexión de emparejamiento de VPC.

Cuando una regla de grupo de seguridad queda obsoleta, esta no se quita automáticamente del grupo de seguridad, sino que debe quitarla manualmente. Si una regla de grupo de seguridad queda obsoleta porque se ha eliminado la interconexión de VPC, esta dejará de marcarse como obsoleto si crea una nueva interconexión de VPC con las mismas VPC.

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.

Para describir las reglas de grupo de seguridad obsoletas mediante la línea de comandos o una API

- [describe-stale-security-groups](#) (AWS CLI)
- [Get-EC2StaleSecurityGroup](#) (AWS Tools for Windows PowerShell)
- [DescribeStaleSecurityGroups](#) (API de consulta de Amazon EC2)

En el ejemplo siguiente, se creó una interconexión entre la VPC A (`vpc-aaaaaaa`) y la VPC B y se eliminó la interconexión de VPC. El grupo de seguridad `sg-aaaa1111` de la VPC A hace referencia al grupo `sg-bbbb2222` de la VPC B. Al ejecutar el comando `describe-stale-security-groups` para su VPC, la respuesta indica que el grupo de seguridad `sg-aaaa1111` tiene una regla SSH obsoleta que hace referencia al grupo `sg-bbbb2222`.

```
aws ec2 describe-stale-security-groups --vpc-id vpc-aaaaaaaa
```

```
{
  "StaleSecurityGroupSet": [
    {
      "VpcId": "vpc-aaaaaaaa",
      "StaleIpPermissionsEgress": [],
      "GroupName": "Access1",
      "StaleIpPermissions": [
        {
          "ToPort": 22,
          "FromPort": 22,
          "UserIdGroupPairs": [
            {
              "VpcId": "vpc-bbbbbbbb",
              "PeeringStatus": "deleted",
              "UserId": "123456789101",
              "GroupName": "Prod1",
              "VpcPeeringConnectionId": "pcx-b04deed9",
              "GroupId": "sg-bbbb2222"
            }
          ],
          "IpProtocol": "tcp"
        }
      ],
      "GroupId": "sg-aaaa1111",
      "Description": "Reference remote SG"
    }
  ]
}
```

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

Modifique las opciones de interconexión de VPC

Para modificar la interconexión de VPC, realice lo siguiente:

- Habilite una o varias instancias de EC2-Classic vinculadas a su VPC mediante ClassicLink para establecer comunicación con las instancias de la VPC del mismo nivel, o bien para habilitar la comunicación de las instancias de su VPC con las instancias de EC2-Classic vinculadas de la VPC del mismo nivel. Para obtener más información, consulte [Configuraciones con ClassicLink \(p. 53\)](#). No es posible habilitar la comunicación de las instancias de EC2-Classic con instancias de una VPC del mismo nivel a través de IPv6.
- Habilite una VPC para que resuelva los nombres de host DNS IPv4 públicos en direcciones IPv4 privadas al realizar consultas desde instancias de la VPC del mismo nivel. Para obtener más información, consulte [Habilite la resolución de DNS para la interconexión de VPC \(p. 15\)](#).

Habilite la resolución de DNS para la interconexión de VPC

Para habilitar una VPC para que resuelva los nombres de host DNS IPv4 públicos en direcciones IPv4 privadas al realizar consultas desde instancias de la VPC interconectada, debe modificar la interconexión existente.

Ambas VPC deben tener habilitados los nombres de host DNS y la resolución de DNS.

No se puede habilitar la compatibilidad con la resolución DNS cuando se crea una nueva interconexión. Puede habilitar la compatibilidad con la resolución DNS para una interconexión existente que esté en el estado `active`.

Para habilitar la resolución de DNS para la interconexión

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections.
3. Seleccione la interconexión de VPC y elija Actions, Edit DNS Settings.
4. Para asegurarse de que las consultas desde la VPC del mismo nivel se resuelvan en direcciones IP privadas en su VPC local, elija la opción para habilitar la resolución de DNS para las consultas que se realizan desde la VPC del mismo nivel. Esta opción es Requester DNS resolution (Resolución DNS del solicitante) o Accepter DNS resolution (Resolución DNS del aceptador), dependiendo de si la VPC es la VPC del solicitante o aceptador.
5. Si la VPC del mismo nivel está en la misma cuenta de AWS, puede habilitar la resolución DNS para ambas VPC en la conexión del mismo nivel.
6. Seleccione Save.
7. Si la VPC interconectada se encuentra en otra cuenta de AWS o en una región diferente, el propietario de esta VPC interconectada deberá iniciar sesión en la consola de VPC, realizar los pasos del 2 al 4 y presionar Save (Guardar).

Para habilitar la resolución de DNS mediante la línea de comandos o una API

- [modify-vpc-peering-connection-options](#) (AWS CLI)
- [Edit-EC2VpcPeeringConnectionOption](#) (AWS Tools for Windows PowerShell)
- [ModifyVpcPeeringConnectionOptions](#) (API de consulta de Amazon EC2)

Deberá modificar las opciones de interconexión de la VPC solicitante si es usted el solicitante de la interconexión de VPC. Deberá modificar las opciones de interconexión de la VPC que acepta la conexión si es usted el responsable de aceptar la interconexión de VPC. Puede utilizar los comandos [describe-vpc-peering-connections](#) o [Get-EC2VpcPeeringConnections](#) para comprobar qué VPC es la que realiza la solicitud de interconexión de VPC y la que la acepta. Para las conexiones interconectadas entre regiones, debe usar la región de la VPC solicitante para modificar las opciones de interconexión de la VPC del solicitante y la región de la VPC receptora para modificar las opciones de interconexión de VPC de la receptora.

En este ejemplo, usted es quien solicita la interconexión de VPC. Por lo tanto, debe modificar las opciones de interconexión mediante AWS CLI tal como se indica a continuación:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --requester-peering-connection-options AllowDnsResolutionFromRemoteVpc=true
```

Elimine la interconexión de VPC

Los propietarios de VPC que intervienen en las interconexiones pueden eliminar la interconexión de VPC en cualquier momento. También puede eliminar interconexiones de VPC que haya solicitado y que sigan con el estado `pending-acceptance`.

No se puede eliminar la interconexión de la VPC cuando la interconexión de la VPC está en el estado `rejected`. Se elimina automáticamente la conexión.

Al eliminar una VPC en la consola de Amazon VPC que forme parte de una interconexión de VPC activa también elimina la interconexión de VPC. Si ha solicitado una interconexión de VPC con una VPC de otra cuenta y elimina su VPC antes de que la otra parte haya aceptado la solicitud, la interconexión de VPC también se eliminará. No podrá eliminar las VPC de las cuales tenga una solicitud `pending-acceptance` de una VPC de otra cuenta. Primero debe rechazar la solicitud de interconexión de VPC.

Cuando se elimina una conexión de pares, el estado se establece como `Deleted`. Cuando la conexión está en este estado, no puede aceptar, rechazar o editar la configuración de DNS.

Para eliminar una interconexión de VPC

1. Abra la consola de Amazon VPC en <https://console.aws.amazon.com/vpc/>.
2. En el panel de navegación, elija Peering Connections.
3. Seleccione la interconexión de VPC y elija Actions, Delete VPC Peering Connection.
4. En el cuadro de diálogo de confirmación, elija Yes, Delete.

Para eliminar una interconexión de VPC mediante la línea de comandos o una API

- [delete-vpc-peering-connection](#) (AWS CLI)
- [Remove-EC2VpcPeeringConnection](#) (AWS Tools for Windows PowerShell)
- [DeleteVpcPeeringConnection](#) (API de consulta de Amazon EC2)

Escenarios de interconexión de VPC

Hay diversos motivos por los que podría necesitar configurar una interconexión con VPC entre sus VPC, o entre una VPC propia y una VPC de una cuenta de AWS distinta. Los siguientes escenarios pueden ayudarle a determinar qué configuración se adapta mejor a sus necesidades de redes.

Situaciones

- [Interconexión de dos o más VPC para proporcionar acceso completo a los recursos \(p. 18\)](#)
- [Interconexión de una VPC para obtener acceso a recursos centralizados \(p. 18\)](#)
- [Interconexión con ClassicLink \(p. 19\)](#)

Interconexión de dos o más VPC para proporcionar acceso completo a los recursos

En este escenario, tiene dos o más VPC que desea interconectar para poder compartir por completo los recursos entre todas las VPC. A continuación se muestran algunos ejemplos:

- Su empresa tiene una VPC para el departamento de finanzas, y otra VPC para el departamento de contabilidad. El departamento de finanzas necesita obtener acceso a todos los recursos del departamento de contabilidad, y el departamento de contabilidad necesita obtener acceso a todos los recursos del departamento de finanzas.
- Su empresa tiene varios departamentos de TI, cada uno con su propia VPC. Algunas VPC se encuentran en la misma cuenta de AWS, mientras que otras están en una cuenta de AWS distinta. Desea interconectar todas las VPC para permitir que los departamentos de TI tengan acceso completo a los recursos de los demás.

Para obtener más información acerca de cómo configurar los ajustes de interconexión con VPC y las tablas de ruteo para este escenario, consulte la siguiente documentación:

- [Utilización de dos VPC interconectadas \(p. 20\)](#)
- [Tres VPC interconectadas \(p. 25\)](#)
- [Varias VPC interconectadas \(p. 31\)](#)

Para obtener más información acerca de la creación y el uso de interconexiones de VPC en la consola de Amazon VPC, consulte [Trabaje con interconexiones de VPC \(p. 6\)](#).

Interconexión de una VPC para obtener acceso a recursos centralizados

En este escenario, dispone de una VPC central que contiene recursos que desea compartir con otras VPC. Su VPC central puede necesitar un acceso completo o parcial a las VPC del mismo nivel y, de forma similar, estas VPC del mismo nivel pueden necesitar un acceso completo o parcial a la VPC central. A continuación se muestran algunos ejemplos:

- El departamento de TI de su empresa tiene una VPC para el uso compartido de archivos. Desea interconectar otras VPC a esa VPC central, pero no desea que las otras VPC se envíen tráfico entre sí.
- Su empresa tiene una VPC que desea compartir con sus clientes. Cada cliente puede crear una interconexión de VPC con su VPC; sin embargo, sus clientes no pueden direccionar el tráfico a otras VPC interconectadas con la suya, ni conocen las rutas de otros clientes.
- Tiene una VPC central que se utiliza para servicios de Active Directory. Las instancias específicas de las VPC del mismo nivel envían solicitudes a los servidores de Active Directory y requieren acceso completo a la VPC central. La VPC central no necesita acceso completo a las VPC del mismo nivel; solo necesita direccionar el tráfico de respuesta a las instancias específicas.

Para obtener más información acerca de cómo configurar los ajustes de interconexión de VPC y las tablas de ruteo para este escenario, consulte los siguientes temas:

- [Una VPC interconectada a dos VPC \(p. 22\)](#)
- [Una VPC interconectada a varias VPC \(p. 27\)](#)
- [Dos VPC interconectadas a dos subredes de una VPC \(p. 40\)](#)
- [Una VPC interconectada a subredes específicas de dos VPC \(p. 45\)](#)
- [Instancias de una VPC interconectada a instancias de dos VPC \(p. 48\)](#)
- [Una VPC interconectada a dos VPC mediante la coincidencia con el prefijo de mayor longitud \(p. 50\)](#)

Para obtener más información acerca de la creación y el uso de interconexiones de VPC en la consola de Amazon VPC, consulte [Trabaje con interconexiones de VPC \(p. 6\)](#).

Interconexión con ClassicLink

Puede modificar una interconexión de VPC para permitir que una o varias instancias de EC2-Classical vinculadas a su VPC mediante ClassicLink se comuniquen con las instancias de la VPC del mismo nivel. De forma similar, puede modificar una interconexión de VPC para permitir que las instancias de su VPC se comuniquen con las instancias vinculadas de EC2-Classical en la VPC del mismo nivel.

Para obtener más información acerca de cómo configurar los ajustes de interconexión de VPC y las tablas de ruteo para este escenario, consulte [Configuraciones con ClassicLink \(p. 53\)](#).

Configuraciones de interconexión de VPC

En la siguiente documentación se describen las configuraciones de interconexión con VPC admitidas. Puede que sea necesaria una configuración que permita el direccionamiento entre el bloque de CIDR completo de cada VPC o bien una configuración que limite el direccionamiento a direcciones IP o subredes específicas.

Configuraciones

- [Configuraciones con rutas a un bloque de CIDR completo \(p. 20\)](#)
- [Configuraciones con rutas específicas \(p. 39\)](#)
- [Configuraciones con ClassicLink \(p. 53\)](#)

Configuraciones con rutas a un bloque de CIDR completo

Puede configurar interconexiones con VPC para que sus tablas de ruteo tengan acceso al bloque de CIDR completo de la VPC del mismo nivel. Para obtener más información acerca de escenarios en los que puede necesitar una configuración de interconexión de VPC específica, consulte [Escenarios de interconexión de VPC \(p. 18\)](#). Para obtener más información acerca de la creación y el uso de interconexiones de VPC en la consola de Amazon VPC, consulte [Trabaje con interconexiones de VPC \(p. 6\)](#).

Configuraciones

- [Utilización de dos VPC interconectadas \(p. 20\)](#)
- [Una VPC interconectada a dos VPC \(p. 22\)](#)
- [Tres VPC interconectadas \(p. 25\)](#)
- [Una VPC interconectada a varias VPC \(p. 27\)](#)
- [Varias VPC interconectadas \(p. 31\)](#)

Utilización de dos VPC interconectadas

Supongamos que tiene una interconexión de VPC (pcx-11112222) entre la VPC A y la VPC B, que se encuentran en la misma cuenta de AWS y no tienen bloques de CIDR solapados.



Puede utilizar este tipo de configuración cuando tiene dos VPC que requieren acceso los recursos de las demás. Por ejemplo, puede configurar la VPC A para los registros de contabilidad y la VPC B para

los registros financieros y establecer que ambas VPC puedan obtener acceso a todos los recursos sin restricciones.

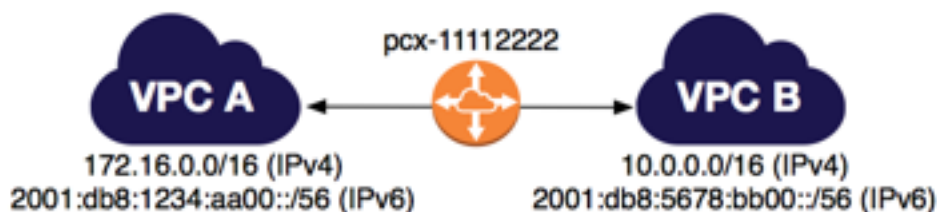
Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC relevante para permitir el acceso al bloque de CIDR completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-11112222
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-11112222

Para obtener más información acerca de la actualización de las tablas de ruteo, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Interconexión de dos VPC para IPv6

Supongamos que tiene las mismas dos VPC en la configuración de interconexión de VPC anterior. En este ejemplo, la VPC A y la VPC B tienen bloques de CIDR IPv6 asociados.



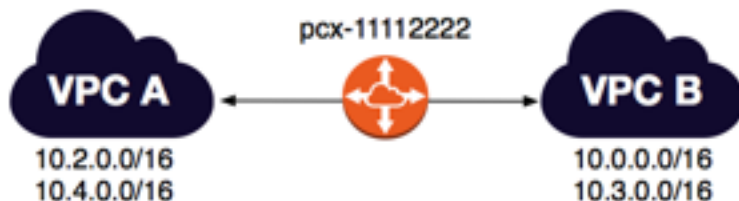
Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC para permitir el acceso al bloque de CIDR IPv6 completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	2001:db8:1234:aa00::/56	Local
	10.0.0.0/16	pcx-11112222
	2001:db8:5678:bb00::/56	pcx-11112222
VPC B	10.0.0.0/16	Local
	2001:db8:5678:bb00::/56	Local
	172.16.0.0/16	pcx-11112222
	2001:db8:1234:aa00::/56	pcx-11112222

Para obtener más información acerca de IPv6 en la VPC, consulte [VPC y subredes](#) en la Guía del usuario de Amazon VPC.

Dos VPC con múltiples CIDR interconectados

Puede añadir bloques de CIDR IPv4 a su VPC. En este ejemplo, la VPC A y la VPC B tienen varios bloques de CIDR IPv4.



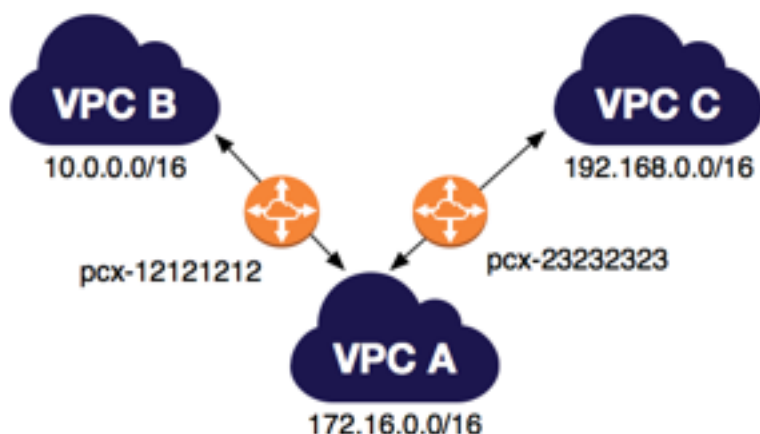
Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC para permitir el acceso a todos los bloques de CIDR IPv4 de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	10.2.0.0/16	Local
	10.4.0.0/16	Local
	10.0.0.0/16	pcx-11112222
	10.3.0.0/16	pcx-11112222
VPC B	10.0.0.0/16	Local
	10.3.0.0/16	Local
	10.2.0.0/16	pcx-11112222
	10.4.0.0/16	pcx-11112222

Para obtener más información, consulte [Agregar bloques de CIDR IPv4 a una VPC](#) en la Guía del usuario de Amazon VPC.

Una VPC interconectada a dos VPC

Supongamos que tiene una VPC central (VPC A) y una interconexión de VPC entre la VPC A y la VPC B (`pcx-12121212`), así como entre la VPC A y la VPC C (`pcx-23232323`). Las VPC se encuentran en la misma cuenta de AWS y no tienen bloques de CIDR solapados.



Puede utilizar esta configuración "triangular" cuando tiene recursos en una VPC central como, por ejemplo un repositorio de servicios, que necesita que estén disponibles para las otras VPC. Las otras VPC no necesitan tener acceso a los recursos de cada una; solo necesitan tener acceso a los recursos de la VPC central.

Note

La VPC B y la VPC C no se pueden enviar tráfico directamente entre sí a través de la VPC A. La interconexión de VPC no admite las relaciones de interconexión transitivas ni el direccionamiento de límite a límite. Por ello debe crear una interconexión de VPC entre la VPC B y la VPC C para poder direccionar el tráfico directamente entre ellas. Para obtener más información, consulte [Tres VPC interconectadas \(p. 25\)](#). Para obtener más información acerca de los escenarios de interconexión no compatibles, consulte [Configuraciones de interconexión de VPC no admitidas \(p. 61\)](#).

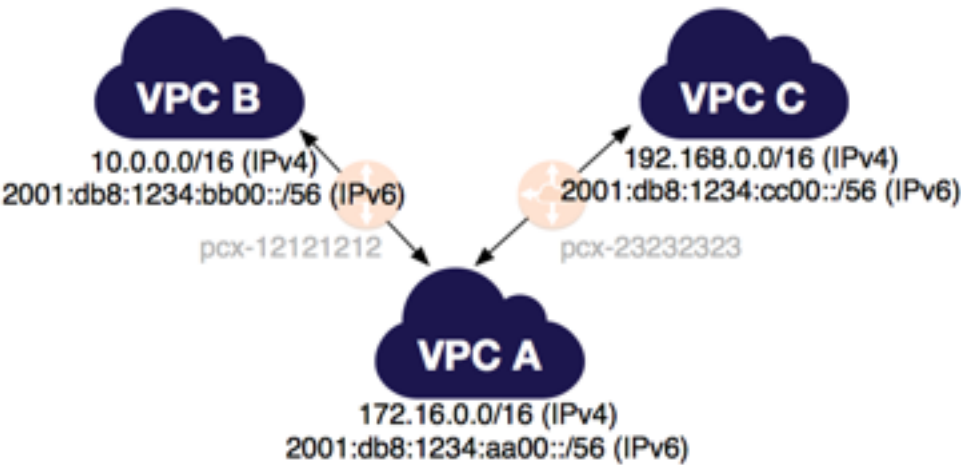
Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC relevante para permitir el acceso al bloque de CIDR completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-12121212
	192.168.0.0/16	pcx-23232323
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-12121212
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-23232323

Para obtener más información acerca de la actualización de las tablas de ruteo, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Una VPC interconectada a dos VPC para IPv6

Supongamos que tiene tres VPC en la configuración de interconexión de VPC anterior. En este ejemplo, las tres VPC tienen bloques de CIDR IPv6 asociados.



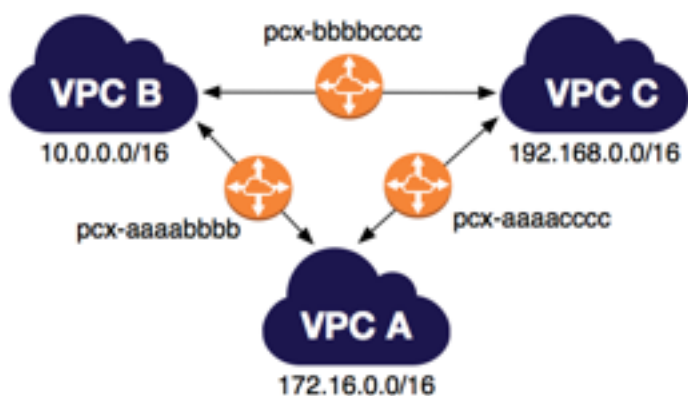
Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC para permitir el acceso al bloque de CIDR IPv6 completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	2001:db8:1234:aa00::/56	Local
	10.0.0.0/16	pcx-12121212
	192.168.0.0/16	pcx-23232323
	2001:db8:1234:bb00::/56	pcx-12121212
	2001:db8:1234:cc00::/56	pcx-23232323
VPC B	10.0.0.0/16	Local
	2001:db8:1234:bb00::/56	Local
	172.16.0.0/16	pcx-12121212
	2001:db8:1234:aa00::/56	pcx-12121212
VPC C	192.168.0.0/16	Local
	2001:db8:1234:cc00::/56	Local
	172.16.0.0/16	pcx-23232323
	2001:db8:1234:aa00::/56	pcx-23232323

Tres VPC interconectadas

Supongamos que tiene interconectadas tres VPC en una configuración de malla completa. Las VPC se encuentran en la misma cuenta de AWS y no tienen bloques de CIDR solapados:

- La VPC A está interconectada a la VPC B a través de la interconexión de VPC `pcx-aaaabbbb`
- La VPC A está interconectada a la VPC C a través de la interconexión de VPC `pcx-aaaacccc`
- La VPC B está interconectada a la VPC C a través de la interconexión de VPC `pcx-bbbbcccc`



Puede utilizar esta configuración de malla completa cuando tiene VPC independientes que deben compartir recursos entre sí sin restricción como, por ejemplo, como sistema de uso compartido de archivos.

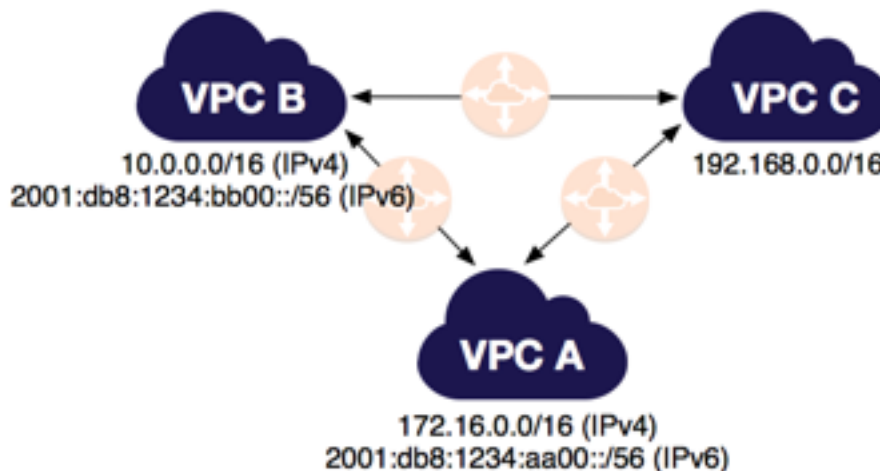
Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC relevante para permitir el acceso al bloque de CIDR completo de las VPC del mismo nivel.

Tablas de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-bbbbcccc
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc
	10.0.0.0/16	pcx-bbbbcccc

Para obtener más información acerca de la actualización de las tablas de ruteo, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Tres VPC interconectadas para IPv6

Supongamos que tiene tres VPC en la configuración de interconexión de VPC anterior. En este ejemplo, la VPC A y la VPC B tienen bloques de CIDR IPv6 asociados. La VPC C no tiene ningún bloque de CIDR IPv6 asociado.



Las tablas de ruteo de la VPC A y la VPC B incluyen rutas que apuntan a la interconexión de VPC `pcx-aaaabbbb` para permitir el acceso al bloque de CIDR IPv6 completo de la VPC del mismo nivel. La VPC A y la VPC B pueden comunicarse mediante IPv6 a través de la interconexión de VPC. La VPC C no puede comunicarse mediante IPv6 ni con la VPC A ni con la VPC B.

Tablas de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	2001:db8:1234:aa00::/56	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
	2001:db8:1234:bb00::/56	pcx-aaaabbbb
VPC B	10.0.0.0/16	Local
	2001:db8:1234:bb00::/56	Local
	172.16.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-bbbbcccc
	2001:db8:1234:aa00::/56	pcx-aaaabbbb
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc
	10.0.0.0/16	pcx-bbbbcccc

El propietario de la VPC C asocia un bloque de CIDR IPv6 con la VPC (2001:db8:1234:cc00::/56). La VPC C no puede comunicarse a través de IPv6 con la VPC A y la VPC B a través de la interconexión de VPC existente. Para ello, debe añadir las siguientes rutas a las tablas de ruteo existentes:

Tablas de ruteo	Destino	Objetivo
VPC A	2001:db8:1234:cc00::/56	pcx-aaaacccc
VPC B	2001:db8:1234:cc00::/56	pcx-bbbbcccc
VPC C	2001:db8:1234:aa00::/56	pcx-aaaaacccc
	2001:db8:1234:bb00::/56	pcx-bbbbcccc

Para obtener más información acerca de IPv6 en la VPC, consulte [VPC y subredes](#) en la Guía del usuario de Amazon VPC.

Una VPC interconectada a varias VPC

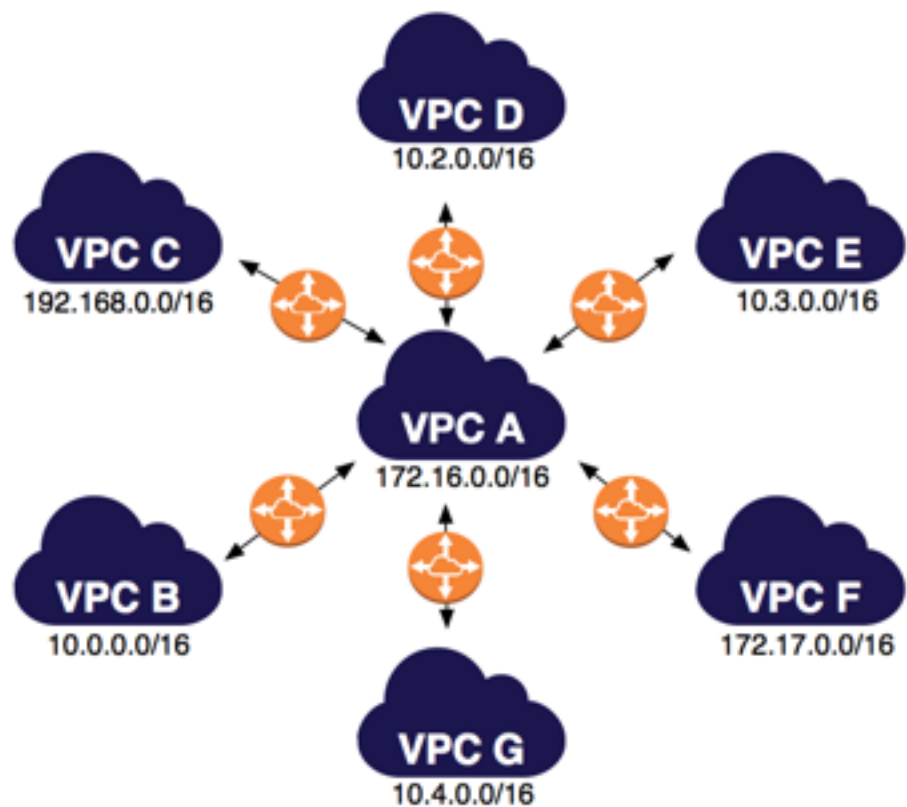
Supongamos que tiene una VPC central (VPC A) interconectada a las siguientes VPC:

- VPC B a través de pcx-aaaabbbb
- VPC C a través de pcx-aaaacccc
- VPC D a través de pcx-aaaadddd
- VPC E a través de pcx-aaaaeeee
- VPC F a través de pcx-aaaaffff
- VPC G a través de pcx-aaaagggg

La VPC A tiene interconexión a todas las demás VPC, pero las demás VPC no están interconectadas entre sí. Las VPC se encuentran en la misma cuenta de AWS y no tienen bloques de CIDR solapados.

Note

Ninguna de las demás VPC puede enviar directamente tráfico a las demás a través de la VPC A. La interconexión de VPC no admite las relaciones de interconexión transitivas ni el direccionamiento de borde a borde. Por ello debe crear una interconexión de VPC entre las demás VPC para poder direccionar el tráfico entre ellas. Para obtener más información, consulte [Varias VPC interconectadas \(p. 31\)](#). Para obtener más información acerca de los escenarios de interconexión no compatibles, consulte [Configuraciones de interconexión de VPC no admitidas \(p. 61\)](#).



Puede utilizar esta configuración "radial" cuando tiene recursos en una VPC central como, por ejemplo un repositorio de servicios, que necesita que estén disponibles para las otras VPC. Las otras VPC no necesitan tener acceso a los recursos de cada una; solo necesitan tener acceso a los recursos de la VPC central.

Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC relevante para permitir el acceso al bloque de CIDR completo de la VPC del mismo nivel.

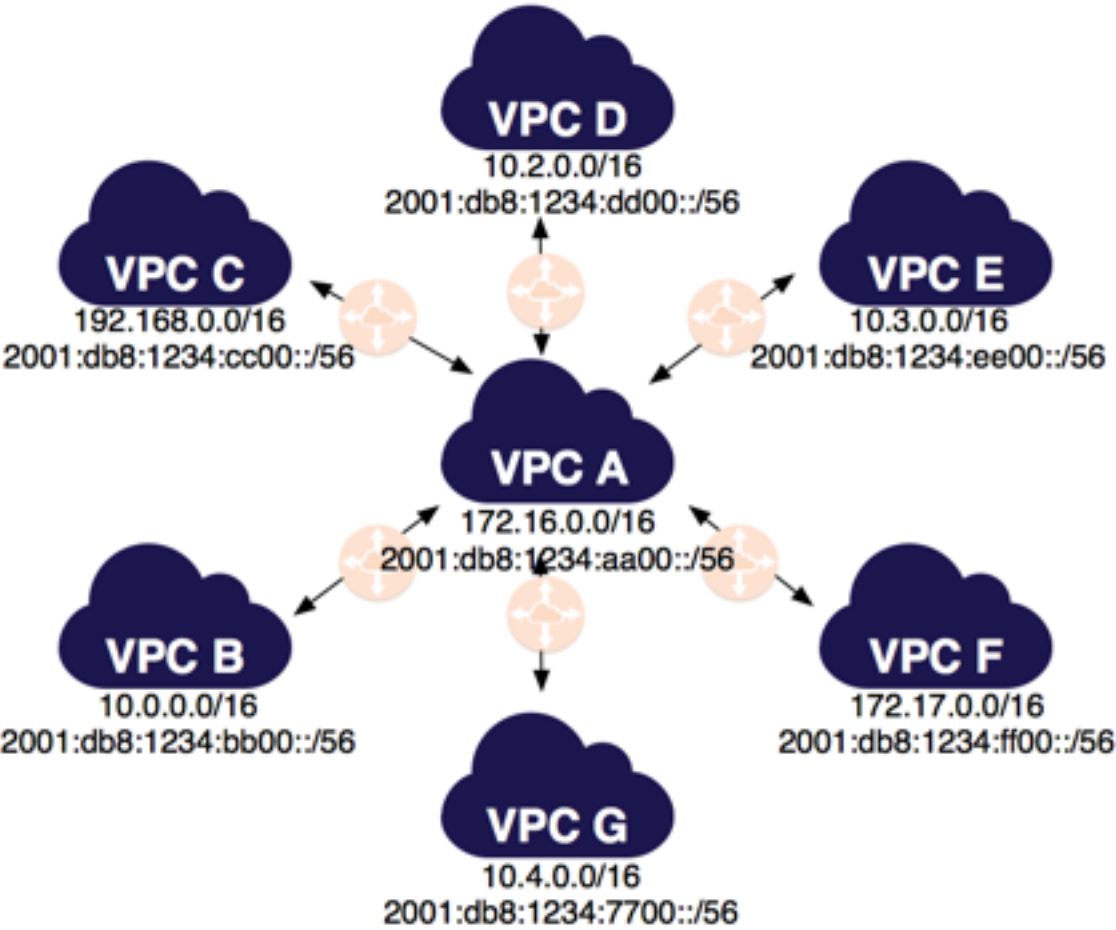
Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
	10.2.0.0/16	pcx-aaaadddd
	10.3.0.0/16	pcx-aaaaeeee
	172.17.0.0/16	pcx-aaaaffff
	10.4.0.0/16	pcx-aaaagggg
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
VPC C	192.168.0.0/16	Local

Tabla de ruteo	Destino	Objetivo
VPC D	172.16.0.0/16	pcx-aaaacccc
	10.2.0.0/16	Local
VPC E	172.16.0.0/16	pcx-aaaadddd
	10.3.0.0/16	Local
VPC F	172.16.0.0/16	pcx-aaaaeeee
	172.17.0.0/16	Local
VPC G	172.16.0.0/16	pcx-aaaaffff
	10.4.0.0/16	Local

Para obtener más información acerca de la actualización de las tablas de ruteo, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Una VPC interconectada a varias VPC para IPv6

Supongamos que tiene las mismas VPC en la configuración de interconexión de VPC anterior. Todas las VPC C tienen bloques de CIDR IPv6 asociados.



Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC relevante para permitir el acceso al bloque de CIDR IPv6 completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	2001:db8:1234:aa00::/56	Local
	10.0.0.0/16	pcx-aaaabbbb
	2001:db8:1234:bb00::/56	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
	2001:db8:1234:cc00::/56	pcx-aaaacccc
	10.2.0.0/16	pcx-aaaadddd
	2001:db8:1234:dd00::/56	pcx-aaaadddd
	10.3.0.0/16	pcx-aaaaeeee
	2001:db8:1234:ee00::/56	pcx-aaaaeeee

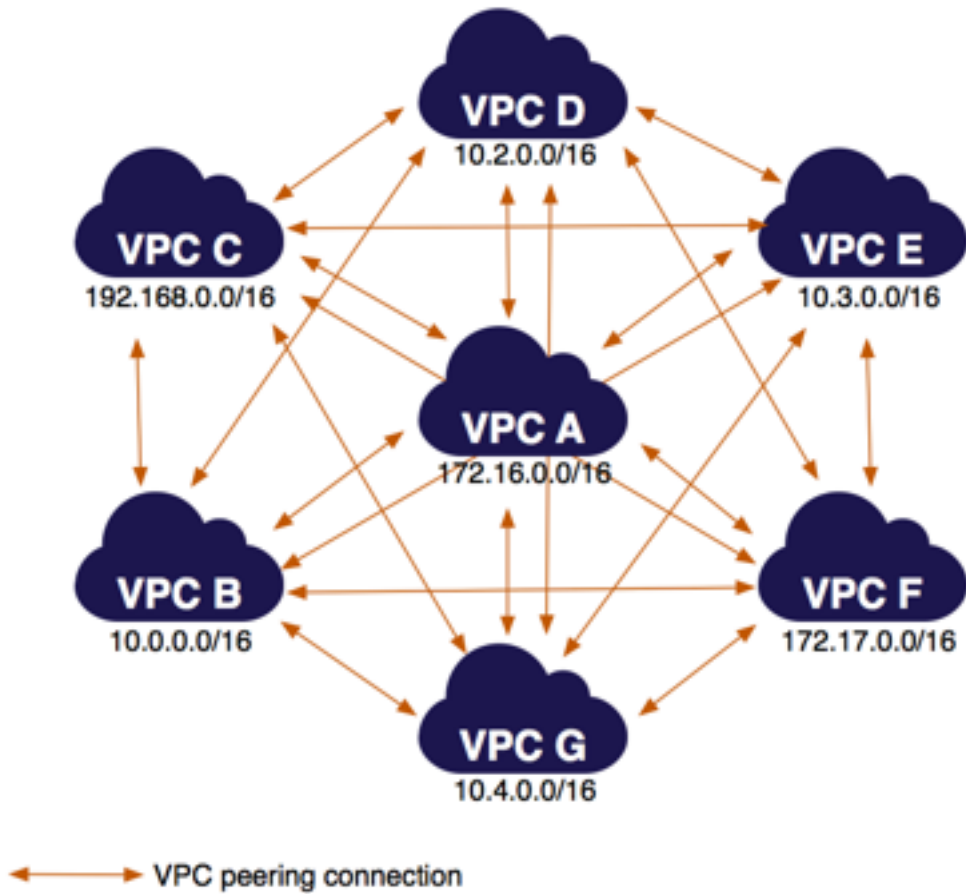
Tabla de ruteo	Destino	Objetivo
	172.17.0.0/16	pcx-aaaaffff
	2001:db8:1234:ff00::/56	pcx-aaaaffff
	10.4.0.0/16	pcx-aaaagggg
	2001:db8:1234:7700::/56	pcx-aaaagggg
VPC B	10.0.0.0/16	Local
	2001:db8:1234:bb00::/56	Local
	172.16.0.0/16	pcx-aaaabbbb
	2001:db8:1234:aa00::/56	pcx-aaaabbbb
VPC C	192.168.0.0/16	Local
	2001:db8:1234:cc00::/56	Local
	172.16.0.0/16	pcx-aaaacccc
	2001:db8:1234:aa00::/56	pcx-aaaacccc
VPC D	10.2.0.0/16	Local
	2001:db8:1234:dd00::/56	Local
	172.16.0.0/16	pcx-aaaadddd
	2001:db8:1234:aa00::/56	pcx-aaaadddd
VPC E	10.3.0.0/16	Local
	2001:db8:1234:ee00::/56	Local
	172.16.0.0/16	pcx-aaaaeeee
	2001:db8:1234:aa00::/56	pcx-aaaaeeee
VPC F	172.17.0.0/16	Local
	2001:db8:1234:ff00::/56	Local
	172.16.0.0/16	pcx-aaaaffff
	2001:db8:1234:aa00::/56	pcx-aaaaffff
VPC G	10.4.0.0/16	Local
	2001:db8:1234:7700::/56	Local
	172.16.0.0/16	pcx-aaaagggg
	2001:db8:1234:aa00::/56	pcx-aaaagggg

Varias VPC interconectadas

Supongamos que tiene interconectadas siete VPC en una configuración de malla completa:

VPC	Interconexión de VPC
A y B	pcx-aaaabbbb
A y C	pcx-aaaacccc
A y D	pcx-aaaadddd
A y E	pcx-aaaaeeee
A y F	pcx-aaaaffff
A y G	pcx-aaaagggg
B y C	pcx-bbbbcccc
B y D	pcx-bbbbdddd
B y E	pcx-bbbbeeee
B y F	pcx-bbbbffff
B y G	pcx-bbbbgggg
C y D	pcx-ccccdddd
C y E	pcx-cccceeee
C y F	pcx-ccccffff
C y G	pcx-ccccgggg
D y E	pcx-ddddeeee
D y F	pcx-ddddffff
D y G	pcx-ddddgggg
E y F	pcx-eeeeffff
E y G	pcx-eeeegggg
F y G	pcx-ffffgggg

Las VPC se encuentran en la misma cuenta de AWS y no tienen bloques de CIDR solapados.



Puede utilizar esta configuración de malla completa cuando tiene varias VPC que deben poder tener acceso a los recursos de las demás sin restricción como, por ejemplo, como red de uso compartido de archivos.

Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC relevante para permitir el acceso al bloque de CIDR completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
	10.2.0.0/16	pcx-aaaadddd
	10.3.0.0/16	pcx-aaaaeeee
	172.17.0.0/16	pcx-aaaaffff
	10.4.0.0/16	pcx-aaaagggg
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb

Amazon Virtual Private Cloud Interconexión de VPC
Varias VPC interconectadas

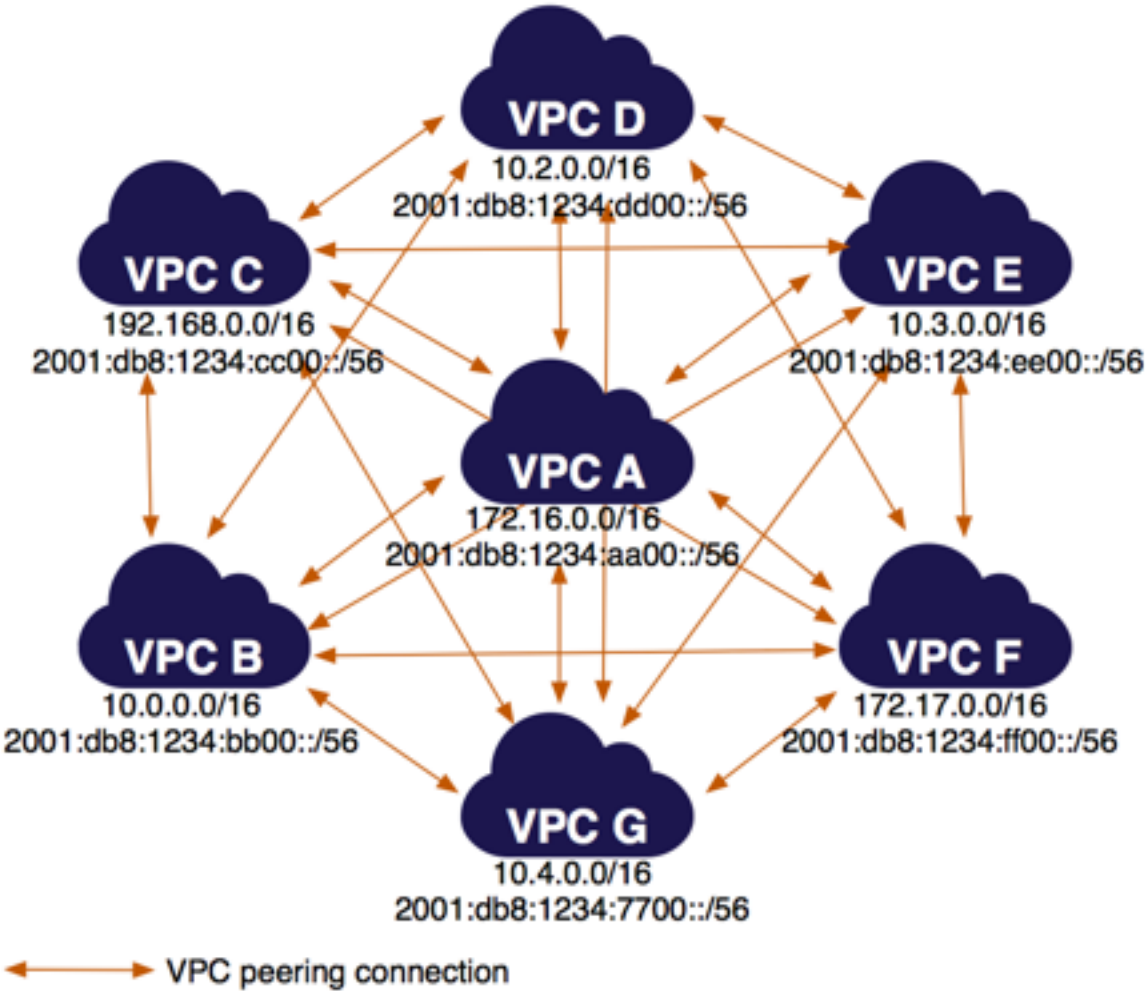
Tabla de ruteo	Destino	Objetivo
	192.168.0.0/16	pcx-bbbbcccc
	10.2.0.0/16	pcx-bbbbdddd
	10.3.0.0/16	pcx-bbbbeeee
	172.17.0.0/16	pcx-bbbbffff
	10.4.0.0/16	pcx-bbbbgggg
VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc
	10.0.0.0/16	pcx-bbbbcccc
	10.2.0.0/16	pcx-ccccdddd
	10.3.0.0/16	pcx-cccceeee
	172.17.0.0/16	pcx-ccccffff
	10.4.0.0/16	pcx-ccccgggg
VPC D	10.2.0.0/16	Local
	172.16.0.0/16	pcx-aaaadddd
	10.0.0.0/16	pcx-bbbbdddd
	192.168.0.0/16	pcx-ccccdddd
	10.3.0.0/16	pcx-ddddeeee
	172.17.0.0/16	pcx-ddddffff
	10.4.0.0/16	pcx-ddddgggg
VPC E	10.3.0.0/16	Local
	172.16.0.0/16	pcx-aaaaeeee
	10.0.0.0/16	pcx-bbbbeeee
	192.168.0.0/16	pcx-cccceeee
	10.2.0.0/16	pcx-ddddeeee
	172.17.0.0/16	pcx-eeeeffff
	10.4.0.0/16	pcx-eeeegggg
VPC F	172.17.0.0/16	Local
	172.16.0.0/16	pcx-aaaaffff
	10.0.0.0/16	pcx-bbbbffff
	192.168.0.0/16	pcx-ccccffff
	10.2.0.0/16	pcx-ddddffff

Tabla de ruteo	Destino	Objetivo
VPC G	10.3.0.0/16	pcx-eeeeffff
	10.4.0.0/16	pcx-ffffgggg
	10.4.0.0/16	Local
	172.16.0.0/16	pcx-aaaagggg
	10.0.0.0/16	pcx-bbbbgggg
	192.168.0.0/16	pcx-ccccgggg
	10.2.0.0/16	pcx-ddddgggg
	10.3.0.0/16	pcx-eeeegggg
	172.17.0.0/16	pcx-ffffgggg

Para obtener más información acerca de la actualización de las tablas de ruteo, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Varias VPC interconectadas para IPv6

Supongamos que tiene las mismas VPC en la configuración de interconexión de VPC anterior. Todas las VPC C tienen bloques de CIDR IPv6 asociados.



Las tablas de ruteo de cada VPC deben apuntar a la interconexión de la VPC para permitir el acceso al bloque de CIDR IPv6 completo de la VPC del mismo nivel.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	2001:db8:1234:aa00::/56	Local
	10.0.0.0/16	pcx-aaaabbbb
	2001:db8:1234:bb00::/56	pcx-aaaabbbb
	192.168.0.0/16	pcx-aaaacccc
	2001:db8:1234:cc00::/56	pcx-aaaacccc
	10.2.0.0/16	pcx-aaaadddd
	2001:db8:1234:dd00::/56	pcx-aaaadddd
	10.3.0.0/16	pcx-aaaaeeee

Amazon Virtual Private Cloud Interconexión de VPC
Varias VPC interconectadas

Tabla de ruteo	Destino	Objetivo
	2001:db8:1234:ee00::/56	pcx-aaaaeene
	172.17.0.0/16	pcx-aaaaffff
	2001:db8:1234:ff00::/56	pcx-aaaaffff
	10.4.0.0/16	pcx-aaaagggg
	2001:db8:1234:7700::/56	pcx-aaaagggg
VPC B	10.0.0.0/16	Local
	2001:db8:1234:bb00::/56	Local
	172.16.0.0/16	pcx-aaaabbbb
	2001:db8:1234:aa00::/56	pcx-aaaabbbb
	192.168.0.0/16	pcx-bbbbcccc
	2001:db8:1234:cc00::/56	pcx-bbbbcccc
	10.2.0.0/16	pcx-bbbbdddd
	2001:db8:1234:dd00::/56	pcx-bbbbdddd
	10.3.0.0/16	pcx-bbbbeeee
	2001:db8:1234:ee00::/56	pcx-bbbbeeee
	172.17.0.0/16	pcx-bbbbffff
	2001:db8:1234:ff00::/56	pcx-bbbbffff
	10.4.0.0/16	pcx-bbbbgggg
	2001:db8:1234:7700::/56	pcx-bbbbgggg
VPC C	192.168.0.0/16	Local
	2001:db8:1234:cc00::/56	Local
	172.16.0.0/16	pcx-aaaacccc
	2001:db8:1234:aa00::/56	pcx-aaaacccc
	10.0.0.0/16	pcx-bbbbcccc
	2001:db8:1234:bb00::/56	pcx-bbbbcccc
	10.2.0.0/16	pcx-ccccdddd
	2001:db8:1234:dd00::/56	pcx-ccccdddd
	10.3.0.0/16	pcx-cccceeee
	2001:db8:1234:ee00::/56	pcx-cccceeee
	172.17.0.0/16	pcx-ccccffff
	2001:db8:1234:ff00::/56	pcx-ccccffff

Amazon Virtual Private Cloud Interconexión de VPC
Varias VPC interconectadas

Tabla de ruteo	Destino	Objetivo
	10.4.0.0/16	pcx-ccccgggg
	2001:db8:1234:7700::/56	pcx-ccccgggg
VPC D	10.2.0.0/16	Local
	2001:db8:1234:dd00::/56	Local
	172.16.0.0/16	pcx-aaaadddd
	2001:db8:1234:aa00::/56	pcx-aaaadddd
	10.0.0.0/16	pcx-bbbbdddd
	2001:db8:1234:bb00::/56	pcx-bbbbdddd
	192.168.0.0/16	pcx-ccccdddd
	2001:db8:1234:cc00::/56	pcx-ccccdddd
	10.3.0.0/16	pcx-ddddeeee
	2001:db8:1234:ee00::/56	pcx-ddddeeee
	172.17.0.0/16	pcx-ddddffff
	2001:db8:1234:ff00::/56	pcx-ddddffff
	10.4.0.0/16	pcx-ddddgggg
	2001:db8:1234:7700::/56	pcx-ddddgggg
VPC E	10.3.0.0/16	Local
	2001:db8:1234:ee00::/56	Local
	172.16.0.0/16	pcx-aaaaeeee
	2001:db8:1234:aa00::/56	pcx-aaaaeeee
	10.0.0.0/16	pcx-bbbbeeee
	2001:db8:1234:bb00::/56	pcx-bbbbeeee
	192.168.0.0/16	pcx-cccceeee
	2001:db8:1234:cc00::/56	pcx-cccceeee
	10.2.0.0/16	pcx-ddddeeee
	2001:db8:1234:dd00::/56	pcx-ddddeeee
	172.17.0.0/16	pcx-eeeeffff
	2001:db8:1234:ff00::/56	pcx-eeeeffff
	10.4.0.0/16	pcx-eeeegggg
	2001:db8:1234:7700::/56	pcx-eeeegggg
VPC F	172.17.0.0/16	Local

Tabla de ruteo	Destino	Objetivo
	2001:db8:1234:ff00::/56	Local
	172.16.0.0/16	pcx-aaaaffff
	2001:db8:1234:aa00::/56	pcx-aaaaffff
	10.0.0.0/16	pcx-bbbbffff
	2001:db8:1234:bb00::/56	pcx-bbbbffff
	192.168.0.0/16	pcx-ccccffff
	2001:db8:1234:cc00::/56	pcx-ccccffff
	10.2.0.0/16	pcx-ddddffff
	2001:db8:1234:dd00::/56	pcx-ddddffff
	10.3.0.0/16	pcx-eeeeffff
	2001:db8:1234:ee00::/56	pcx-eeeeffff
	10.4.0.0/16	pcx-ffffgggg
	2001:db8:1234:7700::/56	pcx-ffffgggg
VPC G	10.4.0.0/16	Local
	2001:db8:1234:7700::/56	Local
	172.16.0.0/16	pcx-aaaagggg
	2001:db8:1234:aa00::/56	pcx-aaaagggg
	10.0.0.0/16	pcx-bbbbgggg
	2001:db8:1234:bb00::/56	pcx-bbbbgggg
	192.168.0.0/16	pcx-ccccgggg
	2001:db8:1234:cc00::/56	pcx-ccccgggg
	10.2.0.0/16	pcx-ddddgggg
	2001:db8:1234:dd00::/56	pcx-ddddgggg
	10.3.0.0/16	pcx-eeeegggg
	2001:db8:1234:ee00::/56	pcx-eeeegggg
	172.17.0.0/16	pcx-ffffgggg
	2001:db8:1234:ff00::/56	pcx-ffffgggg

Configuraciones con rutas específicas

Puede configurar interconexiones con VPC para proporcionar acceso a parte del bloque de CIDR, un bloque de CIDR concreto (si la VPC tiene varios) o a una instancia específica en la VPC del mismo nivel. En estos ejemplos se interconecta una VPC central a una o varias VPC que tienen bloques de

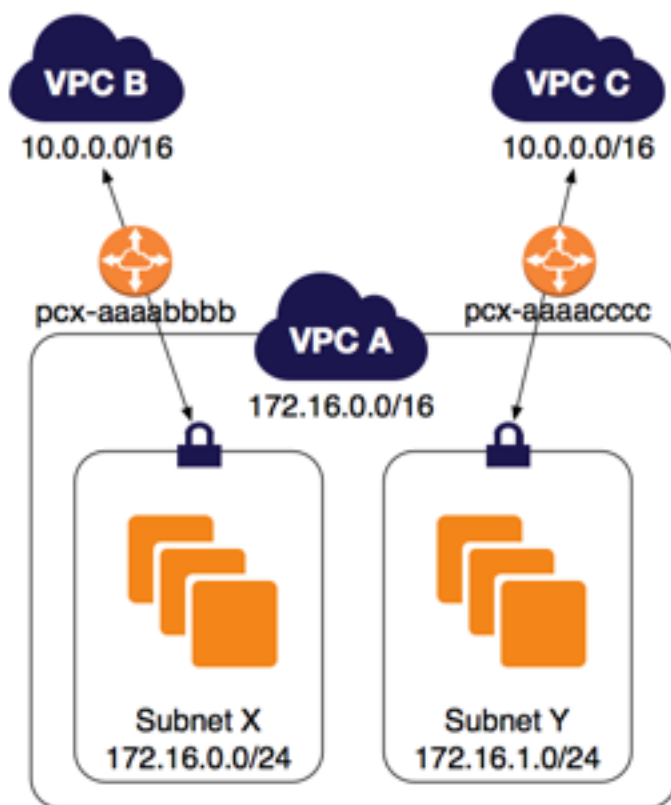
CIDR solapados. Para obtener ejemplos de escenarios en los que puede necesitar una configuración de interconexión de VPC específica, consulte [Escenarios de interconexión de VPC \(p. 18\)](#). Para obtener más información acerca de la creación y el uso de interconexiones de VPC; consulte [Trabaje con interconexiones de VPC \(p. 6\)](#). Para obtener más información acerca de la actualización de las tablas de ruteo, consulte [Actualice sus tablas de enrutamiento para interconexiones de VPC \(p. 10\)](#).

Configuraciones

- [Dos VPC interconectadas a dos subredes de una VPC \(p. 40\)](#)
- [Dos VPC interconectadas a dos bloques de CIDR diferentes en una VPC \(p. 44\)](#)
- [Una VPC interconectada a subredes específicas de dos VPC \(p. 45\)](#)
- [Instancias de una VPC interconectada a instancias de dos VPC \(p. 48\)](#)
- [Una VPC interconectada a dos VPC mediante la coincidencia con el prefijo de mayor longitud \(p. 50\)](#)
- [Múltiples configuraciones de VPC \(p. 51\)](#)

Dos VPC interconectadas a dos subredes de una VPC

Supongamos que tiene una VPC central (VPC A) y una interconexión de VPC entre la VPC A y la VPC B (`pcx-aaaabbbb`), así como entre la VPC A y la VPC C (`pcx-aaaacccc`). La VPC A tiene dos subredes: una para cada interconexión de VPC.



Puede utilizar este tipo de configuración cuando tiene una VPC central con distintos conjuntos de recursos en distintas subredes. Es posible que las otras VPC necesiten obtener acceso a algunos de los recursos, pero no a todos.

La tabla de ruteo de la subred X apunta a la interconexión de VPC `pcx-aaaabbbb` para obtener acceso al bloque de CIDR al completo de la VPC B. La tabla de ruteo de la VPC B apunta a `pcx-aaaabbbb` para obtener acceso al bloque de CIDR solo de la subred X de la VPC A. Del mismo modo, la tabla de ruteo de la subred Y apunta a la interconexión de la VPC `pcx-aaaacccc` para obtener acceso al bloque de CIDR completo de la VPC C. La tabla de ruteo de la VPC C apunta a `pcx-aaaacccc` para obtener acceso al bloque de CIDR solo de la subred Y de la VPC A.

Tabla de ruteo	Destino	Objetivo
Subred X de la VPC A	172.16.0.0/16	Local
	10.0.0.0/16	<code>pcx-aaaabbbb</code>
Subred Y de la VPC A	172.16.0.0/16	Local
	10.0.0.0/16	<code>pcx-aaaacccc</code>
VPC B	10.0.0.0/16	Local
	172.16.0.0/24	<code>pcx-aaaabbbb</code>
VPC C	10.0.0.0/16	Local
	172.16.1.0/24	<code>pcx-aaaacccc</code>

Del mismo modo, la VPC central (VPC A) puede tener varios bloques de CIDR, y las VPC B y C pueden tener una interconexión de VPC a una subred en cada bloque de CIDR.

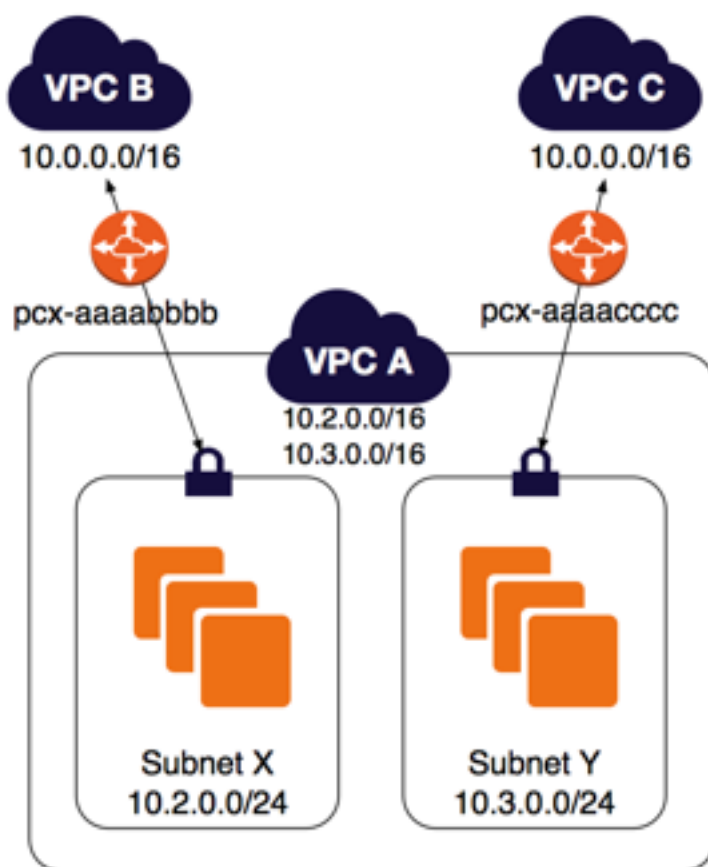
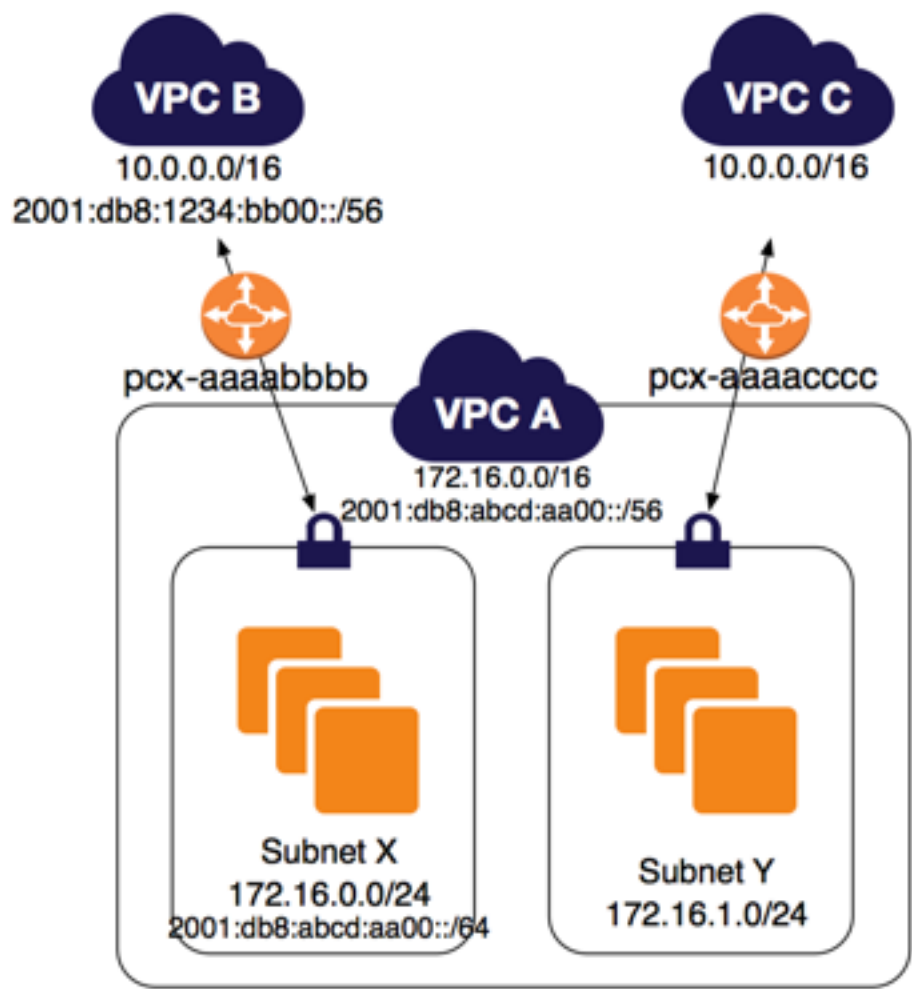


Tabla de ruteo	Destino	Objetivo
Subred X de la VPC A	10.2.0.0/16	Local
	10.3.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
Subred Y de la VPC A	10.2.0.0/16	Local
	10.3.0.0/16	Local
	10.0.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	10.2.0.0/24	pcx-aaaabbbb
VPC C	10.0.0.0/16	Local
	10.3.0.0/24	pcx-aaaacccc

Para obtener más información, consulte [Agregar bloques de CIDR IPv4 a una VPC](#) en la Guía del usuario de Amazon VPC.

Dos VPC interconectadas a dos subredes de una VPC para IPv6

Supongamos que tiene la misma configuración de interconexión de VPC que la que se describe anteriormente. VPC A y VPC B están habilitadas para IPv6, por tanto ambas VPC tienen bloques de CIDR IPv6 asociados. La subred X en la VPC A tiene un bloque de CIDR IPv6 asociado.



Puede habilitar la VPC B para que se pueda comunicar con la subred X de la VPC A a través de IPv6 utilizando la interconexión de VPC. Para ello, añada una ruta a la tabla de ruteo de la VPC A con destino al bloque de CIDR IPv6 para la VPC B, así como una ruta a la tabla de ruteo de la VPC B con destino al bloque CIDR IPv6 de la subred X de la VPC A.

Tabla de ruteo	Destino	Objetivo	Notas
Subred X de la VPC A	172.16.0.0/16	Local	
	2001:db8:abcd:aa00::/56	Local	Ruta local que se añade automáticamente para la comunicación IPv6 en la VPC.
	10.0.0.0/16	pcx-aaaabbbb	
	2001:db8:1234:bb00::/56	pcx-aaaabbbb	Ruta al bloque de CIDR IPv6 de la VPC B.
Subred Y de la VPC A	172.16.0.0/16	Local	

Amazon Virtual Private Cloud Interconexión de VPC
 Dos VPC interconectadas a dos
 bloques de CIDR diferentes en una VPC

Tabla de ruteo	Destino	Objetivo	Notas
VPC B	2001:db8:abcd:aa00::/56	Local	Ruta local que se añade automáticamente para la comunicación IPv6 en la VPC.
	10.0.0.0/16	pcx-aaaacccc	
	10.0.0.0/16	Local	
	2001:db8:1234:bb00::/56	Local	Ruta local que se añade automáticamente para la comunicación IPv6 en la VPC.
VPC C	172.16.0.0/24	pcx-aaaabbbb	
	2001:db8:abcd:aa00::/64	pcx-aaaabbbb	Ruta al bloque de CIDR IPv6 de la VPC A.
	10.0.0.0/16	Local	
	172.16.1.0/24	pcx-aaaacccc	

Dos VPC interconectadas a dos bloques de CIDR diferentes en una VPC

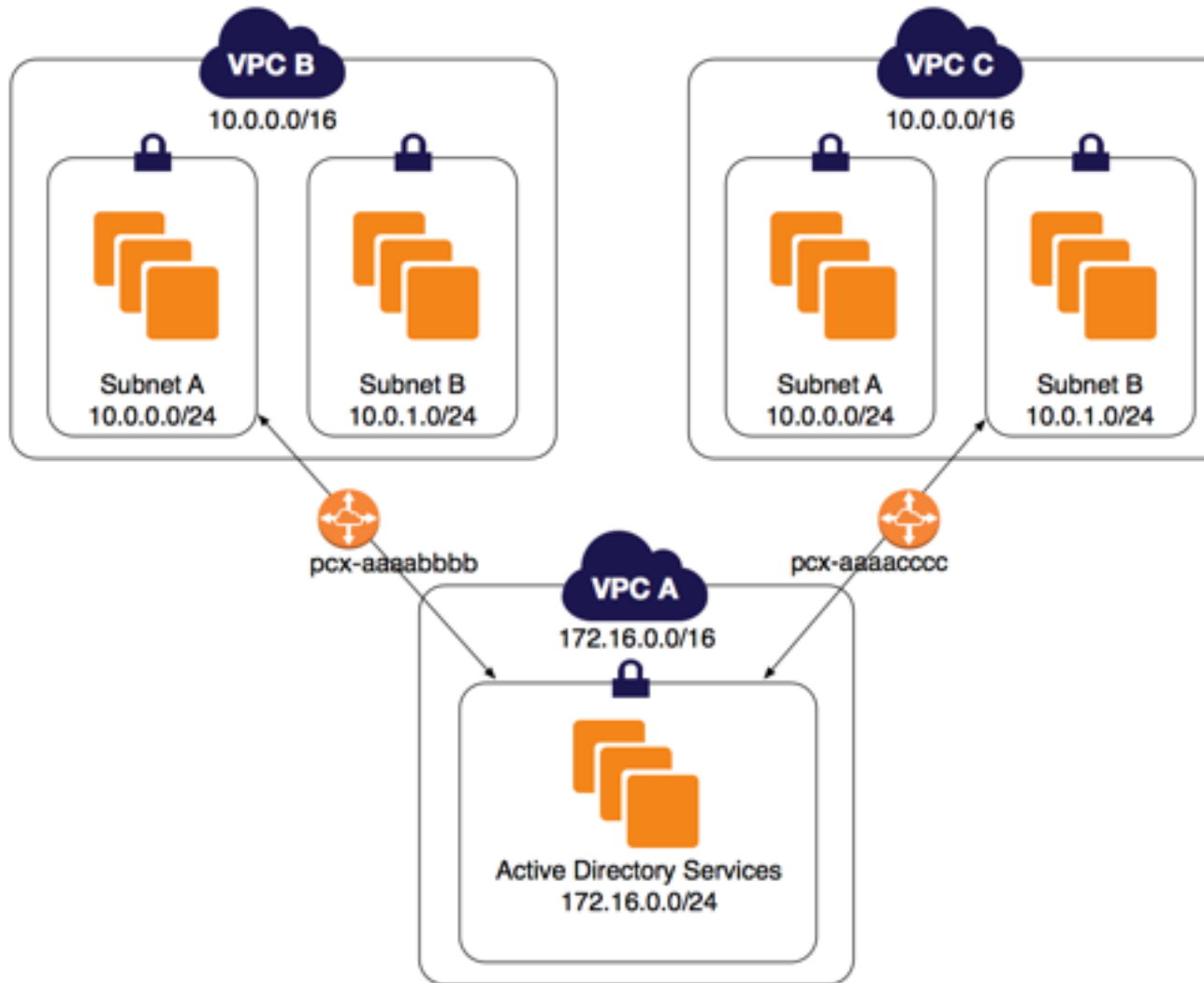
Supongamos que tiene una VPC central (VPC A) y una interconexión de VPC entre la VPC A y la VPC B (pcx-aaaabbbb), así como entre la VPC A y la VPC C (pcx-aaaacccc). La VPC A tiene dos bloques de CIDR: uno para cada interconexión de VPC.

Tabla de ruteo	Destino	Objetivo
VPC A	10.0.0.0/16	Local
	10.2.0.0/16	Local
	172.31.0.0/16	pcx-aaaabbbb
	192.168.0.0/24	pcx-aaaacccc
VPC B	172.31.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
VPC C	192.168.0.0/24	Local
	10.2.0.0/16	pcx-aaaacccc

Para obtener más información, consulte [Agregar bloques de CIDR IPv4 a una VPC](#) en la Guía del usuario de Amazon VPC.

Una VPC interconectada a subredes específicas de dos VPC

Supongamos que tiene una VPC central (VPC A) con una subred y una interconexión de VPC entre la VPC A y la VPC B (pcx-aaaabbbb), así como entre la VPC A y la VPC C (pcx-aaaacccc). La VPC B y la VPC C pueden tener dos subredes cada una y solo una se utiliza para la interconexión con la VPC A.



Puede utilizar este tipo de configuración cuando tenga una VPC central con un único conjunto de recursos como, por ejemplo, servicios de Active Directory, a los que otras VPC necesiten tener acceso. La VPC central no requiere acceso completo a las VPC a las que está interconectada.

La tabla de ruteo de la VPC A apunta a ambas interconexiones de VPC para obtener acceso solo a las subredes específicas de la VPC B y la VPC C. Las tablas de ruteo de las subredes de la VPC B y la VPC C apuntan a sus interconexiones de VPC para obtener acceso a la subred de la VPC A.

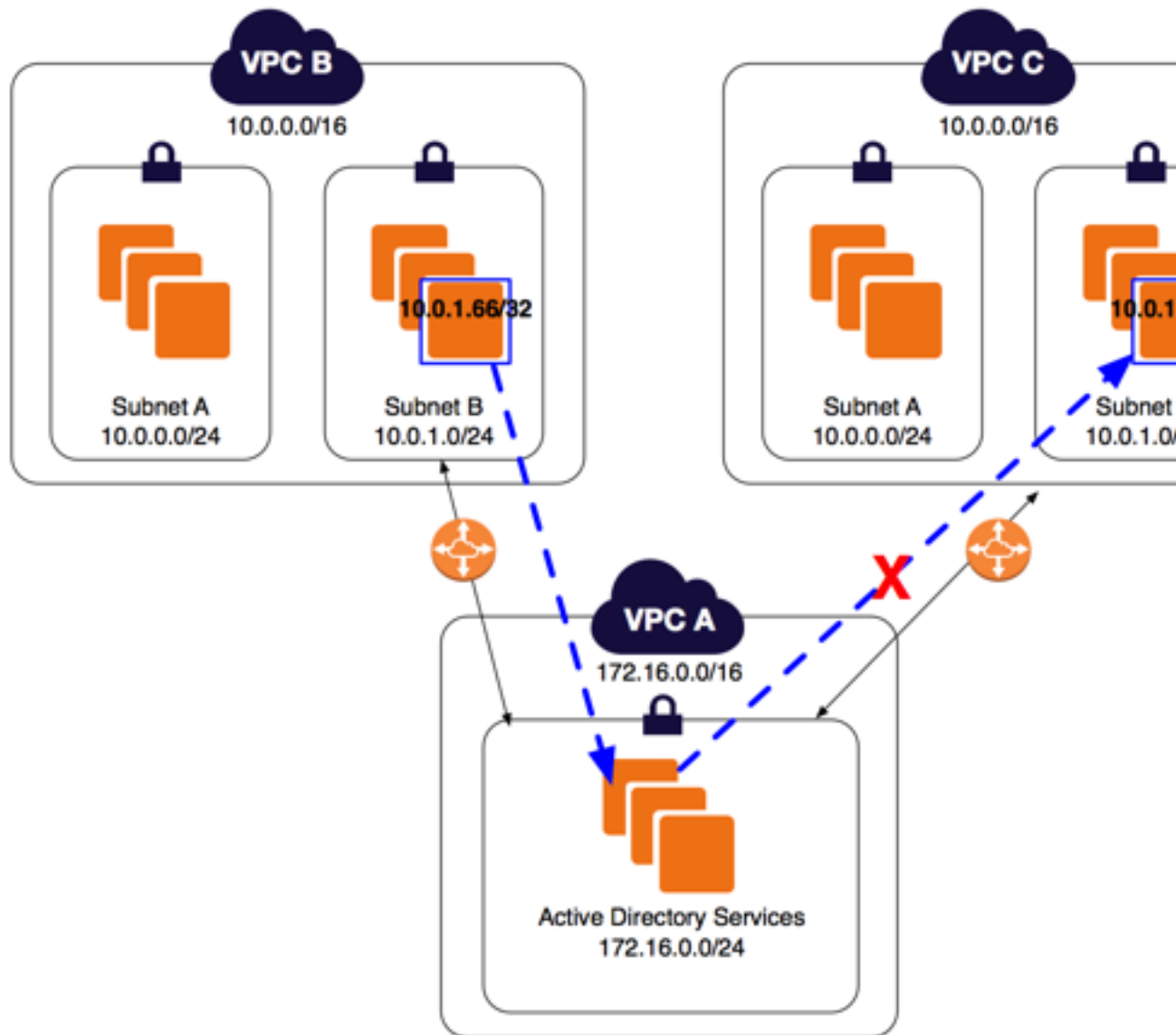
Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/24	pcx-aaaabbbb
	10.0.1.0/24	pcx-aaaacccc
Subred A de la VPC B	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
Subred B de la VPC C	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaacccc

Enrutamiento del tráfico de respuesta

Si tiene una VPC interconectada con varias VPC con bloques de CIDR solapados o que coinciden, asegúrese de que las tablas de ruteo estén configuradas para evitar el envío de tráfico de respuesta desde la VPC a una VPC incorrecta. Actualmente AWS no admite el reenvío de rutas inversas unidifusión en interconexiones de VPC que comprueben la IP de origen de los paquetes y direccionará los paquetes de respuesta de vuelta al origen.

Por ejemplo, la VPC A está interconectada con la VPC B y la VPC C. La VPC B y la VPC C tiene bloques de CIDR coincidentes al igual que sus respectivas subredes. La tabla de ruteo de la subred B de la VPC C apunta a la interconexión de VPC `pcx-aaaabbbb` para obtener acceso a la subred de la VPC A. La tabla de ruteo de la VPC A está configurada para enviar el tráfico `10.0.0.0/16` a la interconexión `pcx-aaaacccc`.

Tabla de ruteo	Destino	Objetivo
Subred B de la VPC B	10.0.0.0/16	Local
	172.16.0.0/24	pcx-aaaabbbb
VPC A	172.16.0.0/24	Local
	10.0.0.0/16	pcx-aaaacccc



Una instancia de la subred B de la VPC C con la dirección IP privada 10.0.1.66/32 envía tráfico al servidor de Active Directory de la VPC A mediante la interconexión de VPC `pcx-aaaabbbb`. La VPC A envía el tráfico de respuesta a 10.0.1.66/32. Sin embargo, la tabla de ruteo de la VPC A está configurada para enviar todo el tráfico del rango de direcciones IP 10.0.0.0/16 a la interconexión de VPC `pcx-aaaacccc`. Si la subred B de la VPC C tiene una instancia con una dirección IP 10.0.1.66/32, esta recibirá el tráfico de respuesta de la VPC A. La instancia de la subred B de la VPC B no recibirá respuesta a las solicitudes que envíe a la VPC A.

Para evitar esto, puede añadir una ruta específica a la tabla de ruteo de la VPC A con destino 10.0.1.0/24 y objetivo `pcx-aaaabbbb`. La ruta del tráfico 10.0.1.0/24 es más específica. Por lo tanto, el tráfico destinado al rango de dirección IP 10.0.1.0/24 se envía a través de la interconexión de VPC `pcx-aaaabbbb`.

De manera alternativa, en el ejemplo siguiente, la tabla de ruteo de la VPC A tiene una ruta para cada subred de cada interconexión de VPC. La VPC A puede comunicarse con la subred B de la VPC B y con la subred A de la VPC C. Este escenario es útil si necesita agregar otra interconexión de VPC con otra

subred que se encuentra en el intervalo de dirección IP 10.0.0.0/16; basta con agregar otra ruta para dicha subred específica.

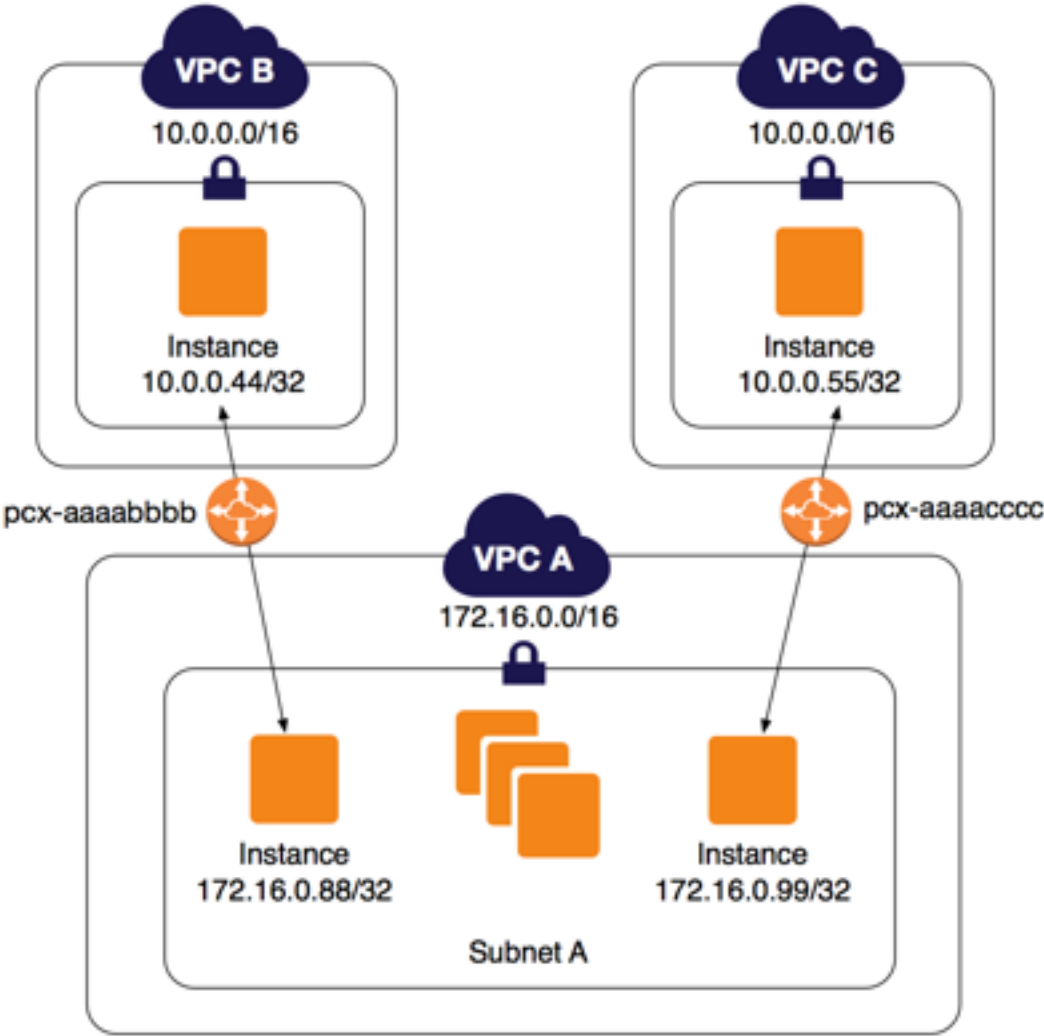
Destino	Objetivo
172.16.0.0/16	Local
10.0.1.0/24	pcx-aaaabbbb
10.0.0.0/24	pcx-aaaacccc

De manera alternativa, dependiendo de su caso, puede crear una ruta a una dirección IP específica de la VPC B para asegurarse de que el tráfico se direcciona de nuevo al servidor correcto (la tabla de ruteo utiliza la coincidencia con el prefijo de mayor longitud para establecer una prioridad en las rutas):

Destino	Objetivo
172.16.0.0/16	Local
10.0.1.66/32	pcx-aaaabbbb
10.0.0.0/16	pcx-aaaacccc

Instancias de una VPC interconectada a instancias de dos VPC

Supongamos que tiene una VPC central (VPC A) con una subred y una interconexión de VPC entre la VPC A y la VPC B (pcx-aaaabbbb), así como entre la VPC A y la VPC C (pcx-aaaacccc). La VPC A tiene una subred que tiene varias instancias; una para cada una de las VPC con las que está interconectada. Puede utilizar este tipo de configuración para limitar el tráfico de interconexión a determinadas instancias.

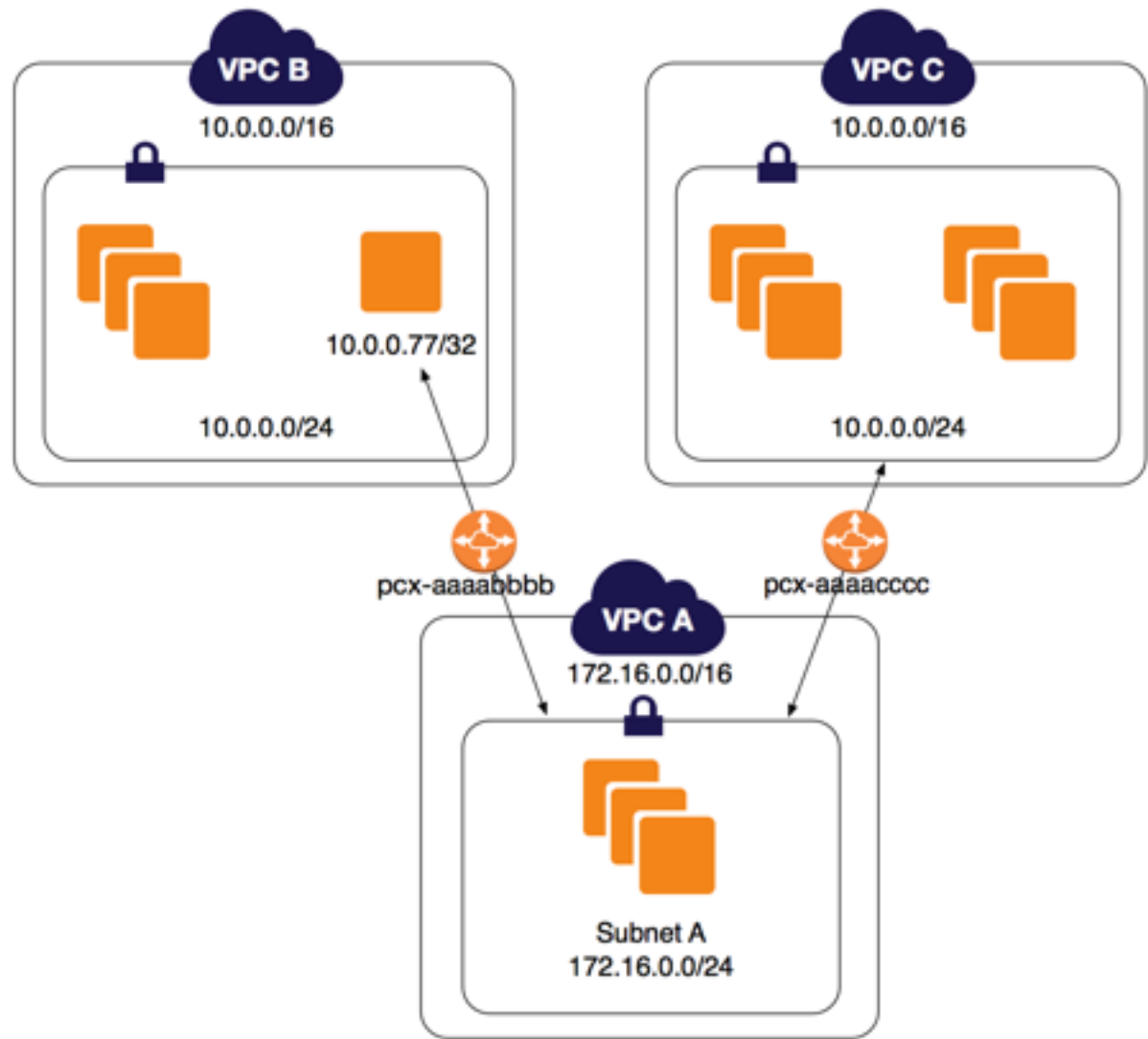


Cada tabla de ruteo de VPC apunta a la interconexión de VPC relevante para obtener acceso a una única dirección IP (y, por lo tanto, a una instancia específica) de la VPC interconectada.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.44/32	pcx-aaaabbbb
	10.0.0.55/32	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.88/32	pcx-aaaabbbb
VPC C	10.0.0.0/16	Local
	172.16.0.99/32	pcx-aaaacccc

Una VPC interconectada a dos VPC mediante la coincidencia con el prefijo de mayor longitud

Supongamos que tiene una VPC central (VPC A) con una subred y una interconexión de VPC entre la VPC A y la VPC B (pcx-aaaabbbb), así como entre la VPC A y la VPC C (pcx-aaaacccc). La VPC B y la VPC C tienen bloques de CIDR coincidentes. Usted desea utilizar la interconexión de VPC pcx-aaaabbbb para direccionar el tráfico entre la VPC A y una instancia específica de la VPC B. El resto del tráfico con destino al rango de dirección IP 10.0.0.0/16 se direcciona mediante pcx-aaaacccc entre la VPC A y la VPC C.



Las tablas de ruteo de la VPC utilizan la coincidencia con el prefijo de mayor longitud para seleccionar la ruta más específica en la interconexión de VPC. El resto del tráfico se direcciona mediante la siguiente ruta coincidente; en este caso, la interconexión de VPC pcx-aaaacccc.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local

Tabla de ruteo	Destino	Objetivo
	10.0.0.77/32	pcx-aaaabbbb
	10.0.0.0/16	pcx-aaaacccc
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
VPC C	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc

Important

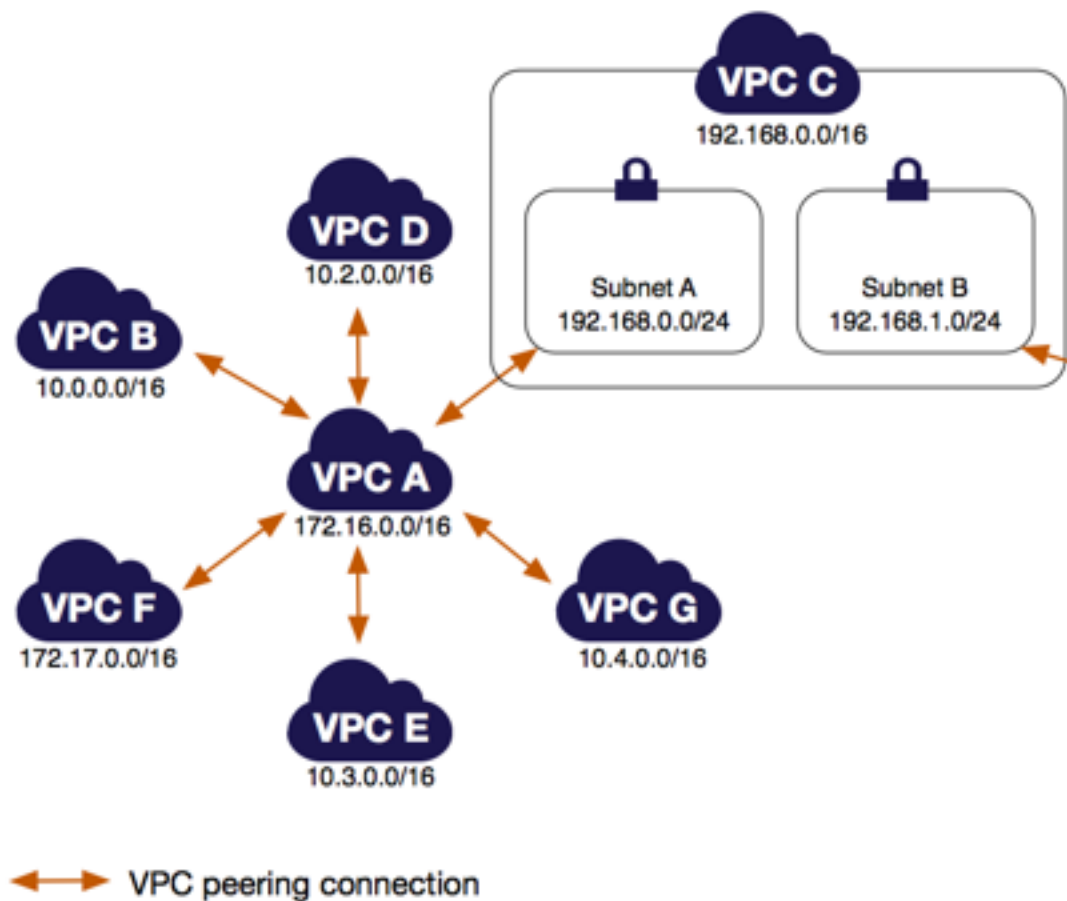
Si una instancia distinta de 10.0.0.77/32 de la VPC B envía tráfico a la VPC A, es posible que el tráfico de respuesta se dirija a la VPC C en lugar de a la VPC B. Para obtener más información, consulte [Enrutamiento del tráfico de respuesta \(p. 46\)](#).

Múltiples configuraciones de VPC

En este ejemplo, una VPC central (VPC A) está interconectada a múltiples VPC en una configuración radial. Para obtener más información acerca de este tipo de configuración, consulte [Una VPC interconectada a varias VPC \(p. 27\)](#). También hay tres VPC (VPC M, N y P) interconectadas entre sí en una configuración de malla completa. Para obtener más información acerca de este tipo de configuración, consulte [Tres VPC interconectadas \(p. 25\)](#).

La VPC C también tiene una interconexión de VPC con la VPC M (pcx-ccccmmmm). La VPC A y la VPC M tienen bloques de CIDR solapados. Esto significa que la interconexión de tráfico entre la VPC A y la VPC C está limitada a una subred específica (subred A) de la VPC C. Esto garantiza que si la VPC C recibe una solicitud de la VPC A o la VPC M, el tráfico de respuesta se enviará a la VPC correcta. Actualmente AWS no admite el reenvío de rutas inversas unidifusión en interconexiones de VPC que comprueben la IP de origen de los paquetes y direccionará los paquetes de respuesta de vuelta al origen. Para obtener más información, consulte [Enrutamiento del tráfico de respuesta \(p. 46\)](#).

Del mismo modo, la VPC C y la VPC P tienen bloques de CIDR solapados. El tráfico de interconexión entre la VPC M y la VPC C está limitado a la subred B de la VPC C y el tráfico de interconexión entre la VPC M y la VPC C está limitado a la subred A de la VPC P. De este modo, se garantiza que si la VPC M recibe tráfico de interconexión de la VPC C o la VPC P, el tráfico de respuesta se enviará de nuevo a la VPC correcta.



Las tablas de ruteo de las VPC B, D, E, F y G apuntan a las interconexiones relevantes para obtener acceso al bloque de CIDR completo de la VPC A. Asimismo, la tabla de ruteo de la VPC A apunta a las interconexiones relevantes de las VPC B, D, E, F y G para obtener acceso a sus bloques de CIDR completos. Para la interconexión `pcx-aaaacccc`, la tabla de ruteo de la VPC A direcciona el tráfico solo a la subred A de la VPC C (192.168.0.0/24) y la tabla de ruteo de la subred A de la VPC C apunta al bloque de CIDR completo de la VPC A.

La tabla de ruteo de la VPC N apunta a las interconexiones relevantes para obtener acceso a los bloques de CIDR al completo de la VPC M y la VPC P. Asimismo, la tabla de ruteo de la VPC P apunta a la interconexión relevante para obtener acceso al bloque de CIDR al completo de la VPC N. La tabla de ruteo de la subred A de la VPC P apunta a la interconexión relevante para obtener acceso al bloque de CIDR al completo de la VPC M. La tabla de ruteo de la VPC M apunta a la interconexión relevante para obtener acceso a la subred B de la VPC C y a la subred A de la VPC P.

Tabla de ruteo	Destino	Objetivo
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-aaaabbbb
	192.168.0.0/24	pcx-aaaacccc
	10.2.0.0/16	pcx-aaaadddd

Tabla de ruteo	Destino	Objetivo
	10.3.0.0/16	pcx-aaaaeerie
	172.17.0.0/16	pcx-aaaaffff
	10.4.0.0/16	pcx-aaaagggg
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-aaaabbbb
Subred A de la VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-aaaacccc
Subred B de la VPC C	192.168.0.0/16	Local
	172.16.0.0/16	pcx-ccccmmmm
VPC D	10.2.0.0/16	Local
	172.16.0.0/16	pcx-aaaadddd
VPC E	10.3.0.0/16	Local
	172.16.0.0/16	pcx-aaaaeerie
VPC F	172.17.0.0/16	Local
	172.16.0.0/16	pcx-aaaaaffff
VPC G	10.4.0.0/16	Local
	172.16.0.0/16	pcx-aaaagggg
VPC M	172.16.0.0/16	Local
	192.168.1.0/24	pcx-ccccmmmm
	10.0.0.0/16	pcx-mmmnnnnn
	192.168.0.0/24	pcx-mmmppppp
VPC N	10.0.0.0/16	Local
	172.16.0.0/16	pcx-mmmnnnnn
	192.168.0.0/16	pcx-nnnppppp
VPC P	192.168.0.0/16	Local
	10.0.0.0/16	pcx-nnnppppp
	172.16.0.0/16	pcx-mmmppppp

Configuraciones con ClassicLink

Si tiene una interconexión con VPC entre dos VPC y hay una o varias instancias de EC2-Classic vinculadas a una o ambas VPC con ClassicLink, podrá ampliar la interconexión de VPC para habilitar la comunicación entre las instancias de EC2-Classic y las instancias de la VPC del otro extremo de la

interconexión con VPC. Esto permite que las instancias de EC2-Classic y las instancias de la VPC se comuniquen mediante direcciones IP privadas. Para ello, habilite una VPC local para que se pueda comunicar con una instancia de EC2-Classic vinculada de una interconexión de VPC, o bien habilite una instancia de EC2-Classic vinculada local para que se pueda comunicar con instancias de VPC en una VPC del mismo nivel.

La comunicación por ClassicLink solo funciona cuando ambas VPC de la interconexión se encuentran en la misma región.

Important

Las instancias de EC2-Classic no admiten la comunicación IPv6. Puede habilitar las instancias de VPC de ambos extremos de la interconexión de VPC para que se comuniquen entre sí mediante IPv6; sin embargo, las instancias de EC2-Classic conectadas mediante ClassicLink a VPC solo pueden comunicarse con instancias de VPC de ambos extremos de la interconexión de VPC mediante IPv4.

Para que la interconexión de VPC admita la comunicación con instancias de EC2-Classic vinculadas, debe modificar las opciones de interconexión de la VPC solicitante, si es usted el solicitante de la interconexión de VPC, o bien debe modificar las opciones de interconexión de VPC aceptante si es usted el responsable de aceptar la interconexión de VPC. Puede utilizar el comando [describe-vpc-peering-connections](#) para comprobar qué VPC es la que acepta y la que solicita la interconexión de VPC.

Siga el proceso siguiente para modificar las opciones de interconexión de VPC:

- Habilite la comunicación entre la instancia de EC2-Classic vinculada local y las instancias de la VPC del mismo nivel.

En este caso, debe modificar las opciones de interconexión de VPC para permitir la comunicación saliente desde la conexión de ClassicLink local a la VPC del mismo nivel en el otro extremo de la interconexión de VPC. El propietario de la VPC del mismo nivel debe modificar las opciones de interconexión de VPC para permitir la comunicación saliente desde sus VPC locales a la conexión de ClassicLink remota.

- Habilite la comunicación entre una VPC local con una instancia de EC2-Classic vinculada de la VPC del mismo nivel.

En este caso, debe modificar las opciones de interconexión de VPC para permitir la comunicación saliente desde su VPC local a la conexión de ClassicLink remota del otro extremo de la interconexión de VPC. El propietario de la VPC del mismo nivel con la instancia de EC2-Classic vinculada debe modificar las opciones de interconexión de la VPC para permitir la comunicación saliente desde su conexión de ClassicLink local a la VPC remota.

Al habilitar la comunicación de una instancia de EC2-Classic vinculada local con instancias de una interconexión de VPC, deberá añadir manualmente una ruta a la tabla de ruteo principal de su VPC local con el destino del bloque de CIDR de la VPC y el objetivo de la interconexión de la VPC. La instancia de EC2-Classic vinculada no se asocia a ningún subconjunto de la VPC y se basa en la tabla de ruteo principal para la comunicación con la VPC del mismo nivel.

Important

La ruta de la interconexión de la VPC debe añadirse a la tabla de ruteo principal independientemente de las tablas de ruteo personalizadas con rutas existentes a la interconexión. De lo contrario, la instancia de EC2-Classic no se podrá comunicar con la VPC del mismo nivel.

Cuando se habilita una VPC local para la comunicación con una conexión de ClassicLink remota, se añade automáticamente una ruta a todas las tablas de ruteo de las VPC locales con destino 10.0.0.0/8 y con el objetivo Local. Esto permite la comunicación con la instancia de EC2-Classic vinculada remota. Si la tabla de ruteo tiene una ruta estática existente en el rango de direcciones IP 10.0.0.0/8 (incluidas las rutas de interconexión de la VPC), no podrá habilitar la comunicación de la VPC local con la conexión de ClassicLink remota.

Compatibilidad de la región

Puede modificar las opciones de interconexión de VPC en las regiones siguientes:

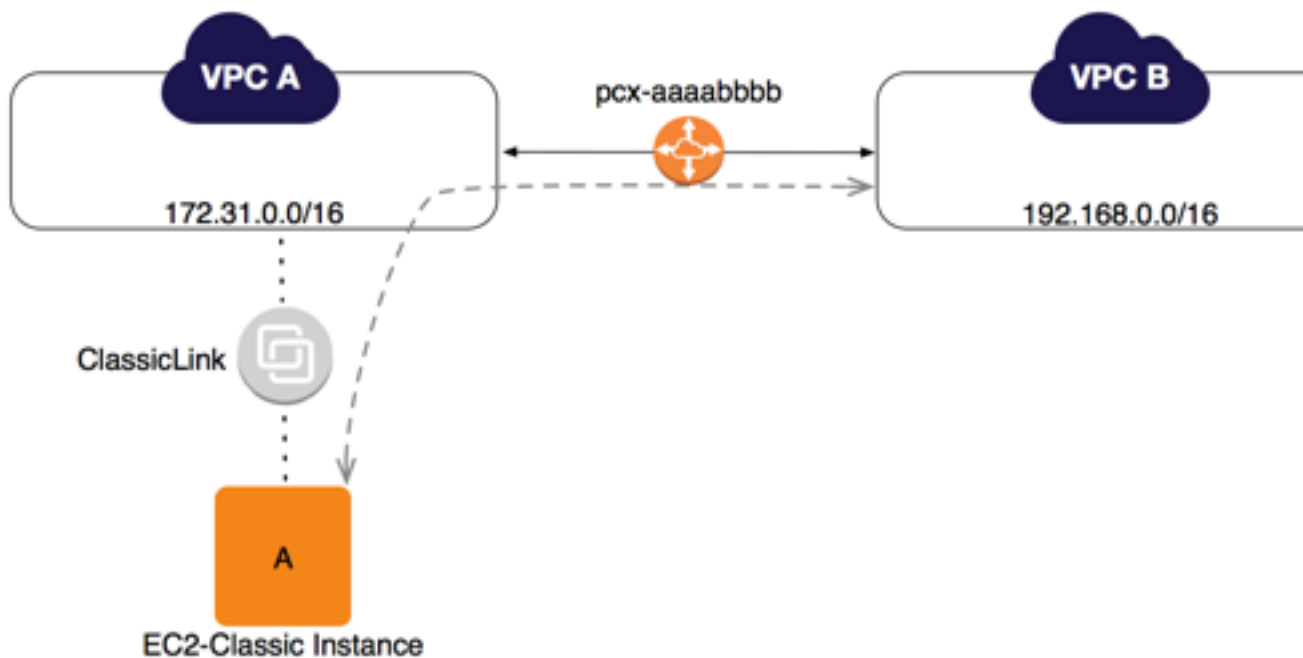
- EE.UU. Este (Norte de Virginia)
- EE.UU. Oeste (Norte de California)
- EE.UU. Oeste (Oregón)
- Europa (Irlanda)
- Asia Pacífico (Tokio)
- Asia Pacífico (Singapur)
- América del Sur (São Paulo)
- Asia Pacífico (Sídney)

Habilitación de la comunicación entre una instancia ClassicLink y una VPC del mismo nivel

En el escenario siguiente, la VPC A está habilitada para ClassicLink y la instancia A se vincula a la VPC A mediante ClassicLink. La VPC B se encuentra en una cuenta de AWS distinta y se interconecta con la VPC A mediante la interconexión de VPC `pcx-aaaabbbb`. La VPC A es la que ha solicitado la interconexión de VPC y la VPC B es la que ha aceptado dicha solicitud. Lo que queremos es que la instancia A se comunique con las instancias de la VPC B a través de IP privadas y que las instancias de la VPC B se comuniquen con la instancia A a través de IP privada.

Note

En este escenario, la VPC B puede ser una VPC de una cuenta compatible con EC2-Classic o una cuenta compatible solo con EC2-VPC.



Las tablas de ruteo de la VPC A contienen rutas para el tráfico de VPC local y rutas que permiten la comunicación con la instancia de EC2-Classic vinculada. La tabla de ruteo personalizada de la VPC A

contiene una ruta que permite que las instancias de la subred se comuniquen con la VPC del mismo nivel a través de una interconexión de VPC, así como una ruta para direccionar todo el tráfico de Internet al puerto de enlace a Internet. La tabla de ruteo personalizada de la VPC B contiene una ruta para permitir que las instancias de la subred se comuniquen con VPC del mismo nivel a través de una interconexión de VPC.

Tabla de ruteo	Destino	Objetivo	Notas
VPC A personalizada	172.31.0.0/16	Local	Ruta local predeterminada para la VPC A.
	192.168.0.0/16	pcx-aaaabbbb	Ruta añadida manualmente para la interconexión entre la VPC A y la VPC B.
	10.0.0.0/8	Local	Ruta añadida manualmente para permitir la comunicación de ClassicLink (añadida al vincular la instancia a la VPC A).
	0.0.0.0/0	igw-11aa22bb	Ruta añadida manualmente para direccionar el tráfico de Internet al puerto de enlace a Internet.
VPC A principal	172.31.0.0/16	Local	Ruta local predeterminada para la VPC A.
	10.0.0.0/8	Local	Ruta añadida manualmente para permitir la comunicación de ClassicLink (añadida al vincular la instancia a la VPC A).
VPC B personalizada	192.168.0.0/16	Local	Ruta local predeterminada para la VPC B.
	172.31.0.0/16	pcx-aaaabbbb	Ruta añadida manualmente para la interconexión entre la VPC A y la VPC B.

El propietario de la VPC A debe modificar la interconexión de VPC para permitir que la instancia A se comuniquen con la VPC B y actualizar la tabla de ruteo principal. El propietario de la VPC B debe modificar la interconexión de VPC para permitir que la VPC B se comuniquen con la instancia A.

Note

Si una VPC se encuentra en una región con EC2-Classic y la otra VPC se encuentra en una región sin EC2-Classic, la opción para actualizar los ajustes de ClassicLink está desactivada en la consola para la región sin EC2-Classic. Por tanto, debe usar la AWS CLI en su lugar.

Tareas

- [Modificación de la interconexión de VPC para la VPC A \(p. 57\)](#)
- [Modificación de la interconexión de VPC para la VPC B \(p. 57\)](#)
- [Visualización de las opciones de interconexión de VPC \(p. 59\)](#)

Modificación de la interconexión de VPC para la VPC A

Para permitir la comunicación desde la instancia de EC2-Classic a la VPC B, el propietario de la cuenta de AWS de la VPC A debe modificar las opciones de interconexión de VPC para permitir que la conexión de ClassicLink local envíe tráfico a las instancias de la VPC del mismo nivel.

Para modificar la interconexión de VPC mediante la consola

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

El propietario de la VPC A debe iniciar sesión en la consola.

2. En el panel de navegación, elija Peering Connections.
3. Seleccione la interconexión de VPC y elija Actions, Edit ClassicLink Settings.
4. Elija la opción para permitir que las instancias de EC2-Classic locales se comuniquen con la VPC del mismo nivel y elija Save.

Para modificar la interconexión de VPC mediante la AWS CLI

Puede utilizar el comando [modify-vpc-peering-connection-options](#). En este caso, la VPC A era la solicitante de la interconexión de VPC; por lo tanto, debe modificar las opciones del solicitante como se muestra a continuación:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --  
requester-peering-connection-options AllowEgressFromLocalClassicLinkToRemoteVpc=true
```

Para actualizar la tabla de ruteo principal

No es necesario realizar cambios en las tablas de ruteo de la VPC B ni en la tabla de ruteo principal de la VPC A. El propietario de la VPC A deberá añadir manualmente una ruta a la tabla de ruteo principal que permite la comunicación de la instancia de EC2-Classic vinculada a través de la interconexión de VPC.

Destino	Objetivo
172.31.0.0/16	Local
10.0.0.0/8	Local
192.168.0.0/16	pcx-aaaabbbb

Para obtener más información acerca de agregar rutas, consulte [Agregar y quitar rutas de una tabla de enrutamiento](#) en la Guía del usuario de Amazon VPC.

Modificación de la interconexión de VPC para la VPC B

A continuación, el propietario de la cuenta de AWS de la VPC B debe modificar las opciones de interconexión de VPC para permitir que la VPC B envíe tráfico a la instancia A de EC2-Classic.

Para modificar la interconexión de VPC mediante la consola

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

El propietario de la VPC B debe iniciar sesión en la consola.

2. En el panel de navegación, elija Peering Connections.
3. Seleccione la interconexión de VPC y elija Actions, Edit ClassicLink Settings.
4. Elija la opción para permitir que las instancias de VPC locales se comuniquen con las instancias de EC2-Classical en la VPC del mismo nivel y elija Save.

Para modificar la interconexión de VPC mediante la AWS CLI

La VPC B ha aceptado la interconexión de VPC; por lo tanto, debe modificar las opciones del aceptador como se muestra a continuación:

```
aws ec2 modify-vpc-peering-connection-options --vpc-peering-connection-id pcx-aaaabbbb --accepter-peering-connection-options AllowEgressFromLocalVpcToRemoteClassicLink=true
```

No es necesario realizar cambios en las tablas de ruteo de la VPC A. Asimismo, se ha añadido automáticamente una nueva ruta a la tabla de ruteo de la VPC B que permite que las instancias de la VPC B se comuniquen con la instancia de EC2-Classical vinculada de la VPC A.

Tabla de ruteo	Destino	Objetivo	Notas
VPC A personalizada	172.31.0.0/16	Local	Ruta local predeterminada para la VPC A.
	192.168.0.0/16	pcx-aaaabbbb	Ruta añadida manualmente para la interconexión entre la VPC A y la VPC B.
	10.0.0.0/8	Local	Ruta añadida manualmente para permitir la comunicación de ClassicLink (añadida al vincular la instancia a la VPC A).
	0.0.0.0/0	igw-11aa22bb	Ruta añadida manualmente para direccionar el tráfico de Internet al puerto de enlace a Internet.
VPC A principal	172.31.0.0/16	Local	Ruta local predeterminada para la VPC A.
	10.0.0.0/8	Local	Ruta añadida manualmente para permitir la comunicación de ClassicLink (añadida al vincular la instancia a la VPC A).

Tabla de ruteo	Destino	Objetivo	Notas
	192.168.0.0/16	pcx-aaaabbbb	Ruta añadida manualmente para permitir que la instancia de EC2-Classical vinculada se comuniquen con la VPC B a través de la interconexión de VPC.
VPC B personalizada	192.168.0.0/16	Local	Ruta local predeterminada para la VPC B.
	172.31.0.0/16	pcx-aaaabbbb	Ruta añadida manualmente para la interconexión entre la VPC A y la VPC B.
	10.0.0.0/8	Local	Ruta añadida manualmente para permitir la comunicación de ClassicLink con la instancia vinculada de la VPC A.

Visualización de las opciones de interconexión de VPC

Puede consultar las opciones de interconexión de VPC de las VPC receptora y solicitante mediante la consola de Amazon VPC o la AWS CLI.

Para ver las opciones de interconexión 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 Peering Connections.
3. Seleccione la interconexión de VPC y elija ClassicLink. Se mostrará la información acerca de las opciones de interconexión de VPC habilitadas o deshabilitadas.

Para ver las opciones de interconexión de VPC mediante la AWS CLI

Puede utilizar el comando `describe-vpc-peering-connections`:

```
aws ec2 describe-vpc-peering-connections --vpc-peering-connection-id pcx-aaaabbbb
```

```
{
  "VpcPeeringConnections": [
    {
      "Status": {
        "Message": "Active",
        "Code": "active"
      },
      "Tags": [
        {
          "Value": "MyPeeringConnection",
          "Key": "Name"
        }
      ]
    }
  ]
}
```

Amazon Virtual Private Cloud Interconexión de VPC
Habilitación de la comunicación entre una
instancia ClassicLink y una VPC del mismo nivel

```
    }
  ],
  "AccepterVpcInfo": {
    "PeeringOptions": {
      "AllowEgressFromLocalVpcToRemoteClassicLink": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowDnsResolutionFromRemoteVpc": false
    },
    "OwnerId": "123456789101",
    "VpcId": "vpc-80cb52e4",
    "CidrBlock": "172.31.0.0/16"
  },
  "VpcPeeringConnectionId": "pcx-aaaabbbb",
  "RequesterVpcInfo": {
    "PeeringOptions": {
      "AllowEgressFromLocalVpcToRemoteClassicLink": false,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": true,
      "AllowDnsResolutionFromRemoteVpc": false
    },
    "OwnerId": "111222333444",
    "VpcId": "vpc-f527be91",
    "CidrBlock": "192.168.0.0/16"
  }
}
]
```

Configuraciones de interconexión de VPC no admitidas

Las siguientes configuraciones de interconexión con VPC no se admiten. En algunos casos puede utilizar una puerta de enlaces de tránsito en lugar de la interconexión. Para obtener más información, consulte [Ejemplos](#) en Gateways de tránsito de Amazon VPC.

Para obtener más información acerca de las limitaciones de interconexión de VPC, consulte [Limitaciones de interconexión de VPC](#) (p. 4).

Configuraciones no válidas

- [Bloques de CIDR solapados](#) (p. 61)
- [Interconexión transitiva](#) (p. 62)
- [Enrutamiento de borde a borde mediante una gateway o una conexión privada](#) (p. 62)

Bloques de CIDR solapados

No puede crear una interconexión de VPC entre VPC que tengan los mismos bloques de CIDR IPv4 o con bloques solapados.



Si las VPC tienen varios bloques de CIDR IPv4, no podrá crear una interconexión de VPC si se superpone cualquiera de los bloques de CIDR (independientemente de que tenga la intención de usar la interconexión de VPC para la comunicación únicamente entre bloques de CIDR que no se superpongan).



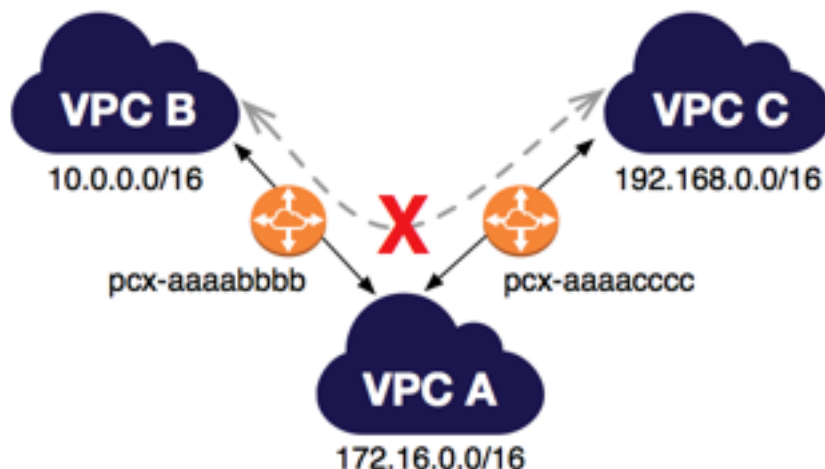
Esta limitación también se aplica a VPC que tienen bloques de CIDR IPv6 que no se solapan. Incluso si pretende utilizar la interconexión de VPC solo para la comunicación IPv6, no podrá crear una interconexión de VPC si las VPC tienen los mismos bloques de CIDR IPv4 o si los bloques se solapan.



Interconexión transitiva

En lugar de usar la interconexión de VPC, puede usar una AWS Transit Gateway que actúe como un centro de tránsito de red para interconectar las redes de las VPC y locales. Para obtener más información acerca de las gateways de tránsito, consulte [Qué es una gateway de tránsito](#) in Gateways de tránsito de Amazon VPC.

Supongamos que tiene una interconexión de VPC entre la VPC A y la VPC B (`pcx-aaaabbbb`) y entre la VPC A y la VPC C (`pcx-aaaacccc`). No hay interconexión de VPC entre la VPC B y la VPC C ni puede direccionar paquetes directamente desde la VPC B a la VPC C a través de la VPC A.



Para direccionar paquetes directamente entre la VPC B y la VPC C, puede crear una interconexión de VPC distinta entre ellas (siempre que no tengan bloques de CIDR solapados). Para obtener más información, consulte [Tres VPC interconectadas](#) (p. 25).

Enrutamiento de borde a borde mediante una gateway o una conexión privada

Si ambas VPC de una relación de interconexión tienen una de las conexiones siguientes, no podrá extender la relación de interconexión a dicha conexión:

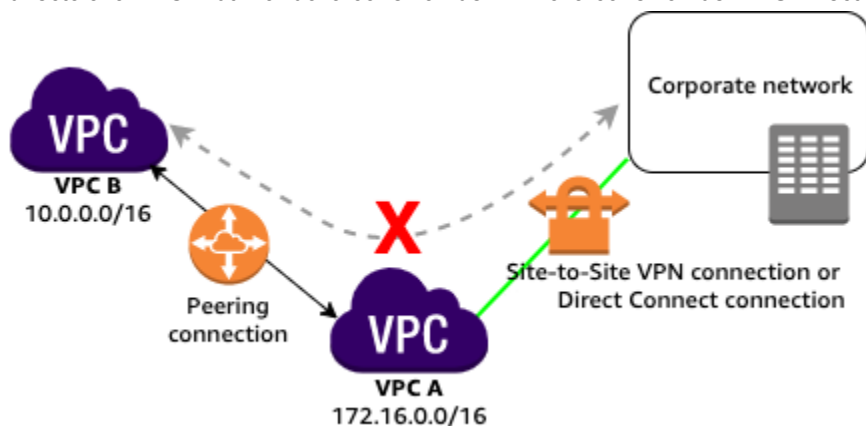
- Conexión de VPN o conexión de AWS Direct Connect a una red corporativa
- Conexión a Internet mediante un puerto de enlace a Internet

- Conexión a Internet de una subred privada mediante un dispositivo NAT
- Un punto de enlace de la VPC de la gateway a un servicio de AWS; por ejemplo, un punto de enlace a Amazon S3.
- (IPv6) Conexión de ClassicLink. Puede habilitar la comunicación IPv4 entre una instancia EC2-Classical enlazada y las instancias de una VPC al otro lado de una conexión de interconexión con VPC. Sin embargo, IPv6 no es compatible con EC2-Classical, por lo que no puede ampliar esta conexión para la comunicación IPv6.

Por ejemplo, si la VPC A y la VPC B están interconectadas y la VPC A tiene alguna de estas conexiones, las instancias de la VPC B no podrán utilizar dicha conexión para obtener acceso a los recursos del otro extremo de la conexión. Del mismo modo, los recursos del otro lado de la conexión no podrán utilizar la conexión para obtener acceso a la VPC B.

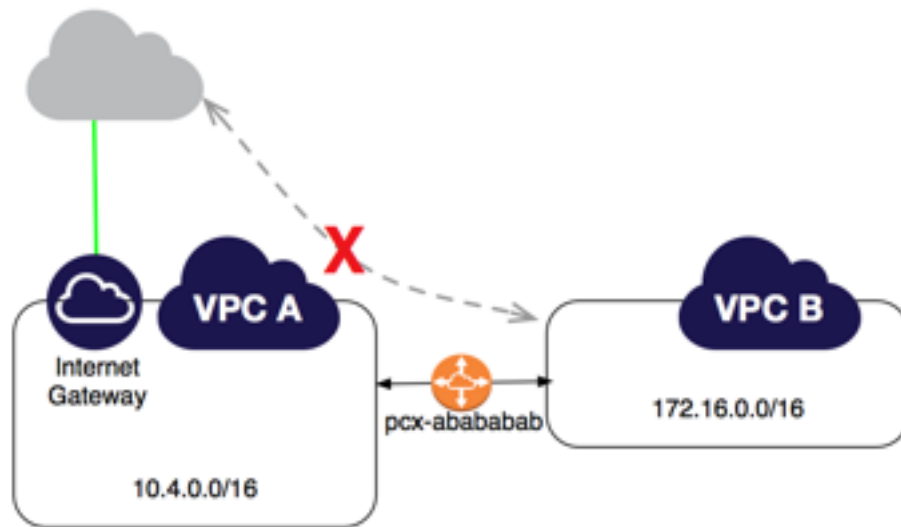
Ejemplo: Enrutamiento de borde a borde mediante una conexión de VPN o una conexión de AWS Direct Connect

Tiene una interconexión de VPC entre VPC A y VPC B. VPC A también tiene una conexión de VPN de sitio a sitio o una conexión de AWS Direct Connect a una red corporativa. Puesto que no se admite el direccionamiento de límite a límite, no podrá utilizar la VPC A para extender la relación de interconexión entre la VPC B y la red corporativa. Por ejemplo, el tráfico de la red corporativa no puede obtener acceso directo a la VPC B utilizando la conexión de VPN o la conexión de AWS Direct Connect a la VPC A.



Ejemplo: Enrutamiento de borde a borde a través de una gateway de Internet

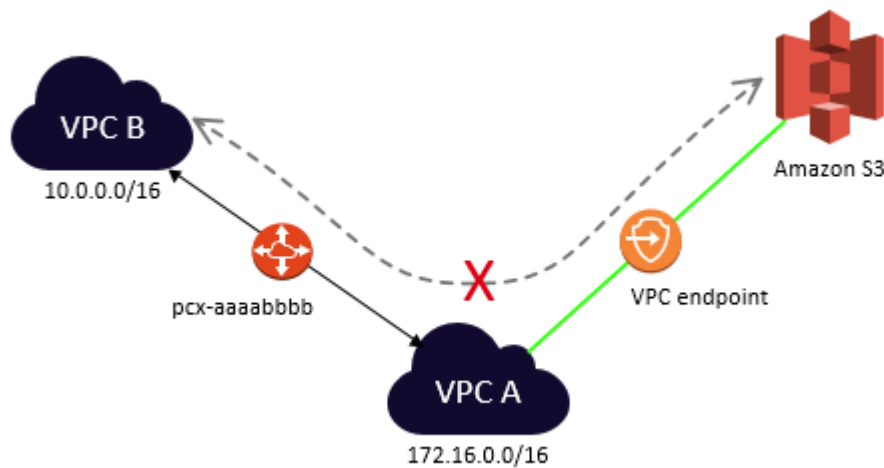
Supongamos que tiene una interconexión de VPC entre la VPC A y la VPC B (pcx-abababab). La VPC A tiene un puerto de enlace a Internet; mientras que la VPC B no. Puesto que no se admite el direccionamiento de límite a límite, no podrá utilizar la VPC A para extender la relación de interconexión entre la VPC B e Internet. Por ejemplo, el tráfico de Internet no puede obtener acceso directo a la VPC B utilizando la conexión del puerto de enlace a Internet a la VPC A.



Del mismo modo, si la VPC A tiene un dispositivo NAT que proporciona acceso a Internet a las instancias de las subredes privadas de la VPC A, las instancias de la VPC B no podrán utilizar el dispositivo NAT para obtener acceso a Internet.

Ejemplo: Enrutamiento de borde a borde a través de un punto de enlace de gateway de la VPC

Supongamos que tiene una interconexión de VPC entre la VPC A y la VPC B (pcx-aaaabbbb). La VPC A tiene un punto de enlace de gateway de VPC que la conecta a Amazon S3. El enrutamiento de borde a borde no es compatible, no puede utilizar la VPC A para extender la relación de interconexión entre la VPC B y Amazon S3. Por ejemplo, la VPC B no puede acceder directamente a Amazon S3 mediante la conexión de punto de enlace de gateway de la VPC a la VPC A.



Administración de identidades y accesos para la interconexión de VPC

De forma predeterminada, los usuarios de IAM no pueden crear ni modificar interconexiones de VPC. Para permitir el acceso a los recursos de interconexiones de VPC, se crea y se asocia una política de IAM a:

- El usuario de IAM o
- El grupo al que pertenece el usuario de IAM.

A continuación, se muestran políticas de IAM de ejemplo para el trabajo con interconexiones de VPC.

Para obtener una lista de las acciones de Amazon VPC y las claves de recursos y condiciones compatibles para cada acción, consulte [Acciones, recursos y claves de condición para Amazon EC2](#) en la Guía del usuario de IAM.

Contenido

- [Creación de una interconexión de VPC](#) (p. 65)
- [Aceptación de una interconexión de VPC](#) (p. 66)
- [Eliminación de una interconexión de VPC](#) (p. 67)
- [Funcionamiento de una cuenta específica](#) (p. 67)
- [Administración de las interconexiones de VPC en la consola](#) (p. 68)

Creación de una interconexión de VPC

La política siguiente permite a los usuarios crear solicitudes de interconexión de VPC utilizando VPC con la etiqueta `Purpose=Peering`. La primera instrucción aplica una clave de condición (`ec2:ResourceTag`) al recurso de la VPC. Tenga en cuenta que el recurso de la VPC de la acción `CreateVpcPeeringConnection` corresponde siempre a la VPC solicitante.

La segunda instrucción concede a los usuarios permisos para crear recursos de interconexión de VPC y, por lo tanto, utiliza el carácter comodín `*` en lugar de un ID de recurso específico.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id:vpc/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/Purpose": "Peering"
      }
    }
  },
  {
    "Effect": "Allow",
```

```
"Action": "ec2:CreateVpcPeeringConnection",
"Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*"
}
]
```

La política siguiente permite a los usuarios de la cuenta de AWS especificada crear interconexiones de VPC mediante cualquier VPC de la región especificada, aunque solo si la VPC que aceptará la interconexión es una VPC determinada en otra cuenta específica.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id-1:vpc/*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
    "Condition": {
      "ArnEquals": {
        "ec2:AcceptorVpc": "arn:aws:ec2:region:account-id-2:vpc/vpc-id"
      }
    }
  }
]
```

Aceptación de una interconexión de VPC

La política siguiente permite a los usuarios aceptar solicitudes de interconexión de VPC provenientes solamente de una cuenta de AWS específica. Esto ayuda a evitar que los usuarios acepten solicitudes de interconexión de VPC de cuentas desconocidas. Esto se consigue al utilizar la clave de condición `ec2:RequesterVpc` en la primera instrucción.

La política también concede a los usuarios permisos para aceptar solicitudes de interconexión solo si su VPC tiene la etiqueta `Purpose=Peering`.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": "ec2:AcceptVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id-1:vpc-peering-connection/*",
    "Condition": {
      "ArnEquals": {
        "ec2:RequesterVpc": "arn:aws:ec2:region:account-id-2:vpc/*"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:AcceptVpcPeeringConnection",
    "Resource": "arn:aws:ec2:region:account-id:vpc/*",
    "Condition": {
      "StringEquals": {
        "ec2:ResourceTag/Purpose": "Peering"
      }
    }
  }
]
```

```
}  
}  
]  
}
```

Eliminación de una interconexión de VPC

La política siguiente permite a los usuarios de la cuenta especificada eliminar cualquier interconexión de VPC, salvo aquellas que utilicen la VPC especificada, que se encuentra en la misma cuenta. La política especifica las claves de condición `ec2:AcceptorVpc` y `ec2:RequesterVpc`, ya que es posible que la VPC haya sido la VPC solicitante o la VPC del mismo nivel en la solicitud de interconexión de VPC original.

```
{  
  "Version": "2012-10-17",  
  "Statement": [{  
    "Effect": "Allow",  
    "Action": "ec2:DeleteVpcPeeringConnection",  
    "Resource": "arn:aws:ec2:region:account-id:vpc-peering-connection/*",  
    "Condition": {  
      "ArnNotEquals": {  
        "ec2:AcceptorVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id",  
        "ec2:RequesterVpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"  
      }  
    }  
  }  
]  
}
```

Funcionamiento de una cuenta específica

La política siguiente permite a los usuarios usar interconexiones de VPC de una cuenta específica. La política permite a los usuarios ver, crear, aceptar, rechazar y eliminar interconexiones de VPC siempre que se encuentren en la misma cuenta de AWS.

La primera instrucción permite a los usuarios ver todas las interconexiones de VPC. El elemento `Resource` requiere el carácter comodín `*` en este caso, ya que la acción de la API (`DescribeVpcPeeringConnections`) no admite actualmente los permisos de nivel de recurso.

La segunda instrucción permite a los usuarios crear interconexiones de VPC y permite para ello el acceso a todas las VPC de la cuenta especificada.

La tercera instrucción utiliza el carácter comodín `*` como parte del elemento `Action` para permitir todas las acciones de interconexión de VPC. Las claves de condición aseguran que las acciones solo se puedan realizar en interconexiones de VPC con VPC que forman parte de la cuenta. Por ejemplo, un usuario no podrá eliminar una interconexión de VPC si la VPC solicitante o responsable de aceptar la solicitud se encuentran en cuentas distintas. Los usuarios no podrán crear interconexiones de VPC con VPC de otras cuentas distintas.

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

```
"Effect": "Allow",
"Action": ["ec2:CreateVpcPeeringConnection", "ec2:AcceptVpcPeeringConnection"],
"Resource": "arn:aws:ec2:*:account-id:vpc/*"
},
{
  "Effect": "Allow",
  "Action": "ec2:*VpcPeeringConnection",
  "Resource": "arn:aws:ec2:*:account-id:vpc-peering-connection/*",
  "Condition": {
    "ArnEquals": {
      "ec2:AcceptorVpc": "arn:aws:ec2:*:account-id:vpc/*",
      "ec2:RequesterVpc": "arn:aws:ec2:*:account-id:vpc/*"
    }
  }
}
]
```

Administración de las interconexiones de VPC en la consola

Para consultar las interconexiones de VPC en la consola de Amazon VPC, los usuarios deben tener permiso para utilizar la acción `ec2:DescribeVpcPeeringConnections`. Para poder utilizar la página `Create Peering Connection` (Crear interconexiones), los usuarios deben tener permiso para utilizar la acción `ec2:DescribeVpcs`. Esto les permite visualizar y seleccionar una VPC. Puede aplicar permisos de nivel de recurso a todas las acciones `ec2:*PeeringConnection` excepto `ec2:DescribeVpcPeeringConnections`.

La política siguiente permite a los usuarios ver interconexiones de VPC y utilizar el cuadro de diálogo `Create VPC Peering Connection` (Crear interconexiones de VPC) para crear una interconexión de VPC que utilice solo una VPC solicitante específica. Si los usuarios intentan crear una interconexión de VPC con una VPC solicitante distinta, se producirá un error en la solicitud.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeVpcPeeringConnections", "ec2:DescribeVpcs"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateVpcPeeringConnection",
    "Resource": [
      "arn:aws:ec2:*:vpc/vpc-id",
      "arn:aws:ec2:*:vpc-peering-connection/*"
    ]
  }
]
```

Historial de revisión

Para obtener más información acerca de los cambios importantes en cada versión de la Guía de interconexión de Amazon VPC, consulte [Historial de documentos](#) en la Guía del usuario de Amazon VPC.