



Google Cloud y la arquitectura de redes híbridas

Philipp Maier
Desarrollador de cursos, Google Cloud

En este módulo, analizaremos las arquitecturas de red de Google Cloud, incluidas las arquitecturas híbridas.

Objetivos de aprendizaje

- Diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento
- Configurar balanceadores de cargas globales y regionales para proporcionar acceso a los servicios
- Usar Cloud CDN para reducir la latencia y la salida de red
- Evaluar la arquitectura de red con Network Intelligence Center
- Conectar redes mediante el intercambio de tráfico, las VPN y Cloud Interconnect

Comenzaremos por ver cómo diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento. Luego, abordaremos la configuración de balanceadores de cargas globales y regionales para proporcionar acceso a servicios.

Como parte de la configuración del balanceador de cargas, puede habilitar Cloud CDN para reducir la latencia y la salida de red, lo que disminuye los costos de las herramientas de redes. También presentaremos Network Intelligence Center, que permite evaluar la arquitectura de la red, y revisaremos las opciones de conexión de red, incluidos el intercambio de tráfico, la VPN y Cloud Interconnect.

Objetivos de aprendizaje

- Diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento
- Configurar balanceadores de cargas globales y regionales para proporcionar acceso a los servicios
- Usar Cloud CDN para reducir la latencia y la salida de red
- Evaluar la arquitectura de red con Network Intelligence Center
- Conectar redes mediante el intercambio de tráfico, las VPN y Cloud Interconnect

Comenzaremos por ver cómo diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento.

Objetivos de aprendizaje

- Diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento
- Configurar balanceadores de cargas globales y regionales para proporcionar acceso a los servicios
- Usar Cloud CDN para reducir la latencia y la salida de red
- Evaluar la arquitectura de red con Network Intelligence Center
- Conectar redes mediante el intercambio de tráfico, las VPN y Cloud Interconnect

Luego, abordaremos la configuración de balanceadores de cargas globales y regionales para proporcionar acceso a servicios.

Objetivos de aprendizaje

- Diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento
- Configurar balanceadores de cargas globales y regionales para proporcionar acceso a los servicios
- Usar Cloud CDN para reducir la latencia y la salida de red
- Evaluar la arquitectura de red con Network Intelligence Center
- Conectar redes mediante el intercambio de tráfico, las VPN y Cloud Interconnect

Como parte de la configuración del balanceador de cargas, puede habilitar Cloud CDN para reducir la latencia y la salida de red, lo que disminuye los costos de las herramientas de redes.

Objetivos de aprendizaje

- Diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento
- Configurar balanceadores de cargas globales y regionales para proporcionar acceso a los servicios
- Usar Cloud CDN para reducir la latencia y la salida de red
- Evaluar la arquitectura de red con Network Intelligence Center
- Conectar redes mediante el intercambio de tráfico, las VPN y Cloud Interconnect

También presentaremos Network Intelligence Center, que permite evaluar la arquitectura de la red...

Objetivos de aprendizaje

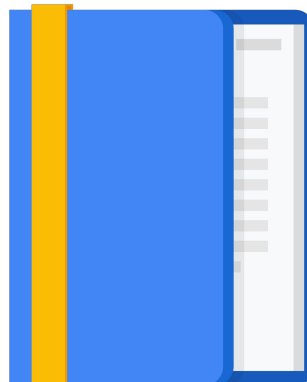
- Diseñar redes de VPC para aplicar optimizaciones a fin de mejorar el costo, la seguridad y el rendimiento
- Configurar balanceadores de cargas globales y regionales para proporcionar acceso a los servicios
- Usar Cloud CDN para reducir la latencia y la salida de red
- Evaluar la arquitectura de red con Network Intelligence Center
- Conectar redes mediante el intercambio de tráfico, las VPN y Cloud Interconnect

y revisaremos las opciones de conexión de red, incluidos el intercambio de tráfico, la VPN y Cloud Interconnect.

Temario

Diseñe redes de Google Cloud

Conecte redes



Comencemos por diseñar redes y balanceadores de cargas de Google Cloud.

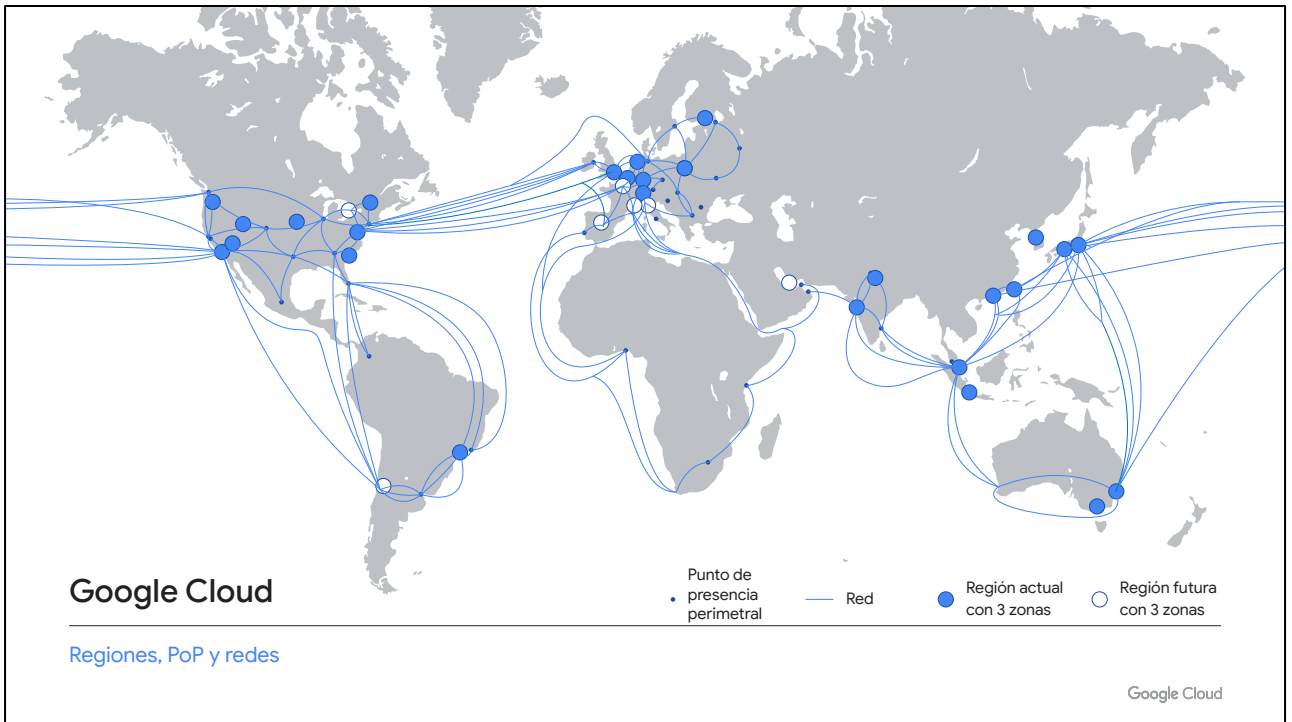
Google mantiene una red global que conecta distintas regiones del mundo

Diseñe sus redes según la ubicación, la cantidad de usuarios, la escalabilidad, la tolerancia a errores y otros requisitos de los servicios.



Google mantiene una red global que conecta distintas regiones del mundo. Puede utilizar esta infraestructura que tiene un alto ancho de banda para diseñar sus redes en la nube a fin de cumplir con requisitos como la ubicación, la cantidad de usuarios, la escalabilidad, la tolerancia a errores y la latencia.

Analicemos con más detalle la red de Google Cloud.



Este mapa representa el alcance de Google Cloud. En general, Google Cloud consta de regiones (íconos azules), puntos de presencia o PoP (puntos pequeños), una red privada global (líneas azules) y servicios.

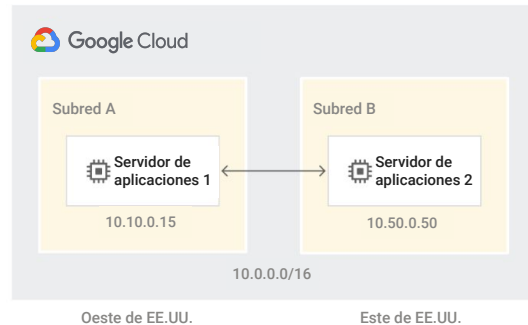
Una región es una ubicación geográfica específica donde puede ejecutar sus recursos. En este mapa, se muestran varias regiones que operan en la actualidad y aquellas que lo harán en el futuro con sus respectivas zonas. En el momento de esta presentación, hay 21 regiones y 64 zonas.

Los PoP son lugares donde la red de Google se conecta al resto de Internet. Google Cloud puede acercar su tráfico al de sus pares porque opera una amplia red global de puntos de interconexión, lo que permite reducir los costos y proporcionar una mejor experiencia a los usuarios.

La red conecta regiones y PoP, y se compone de una red global de cables de fibra óptica con varias inversiones en cables submarinos.

En Google Cloud, las redes de VPC son globales

- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



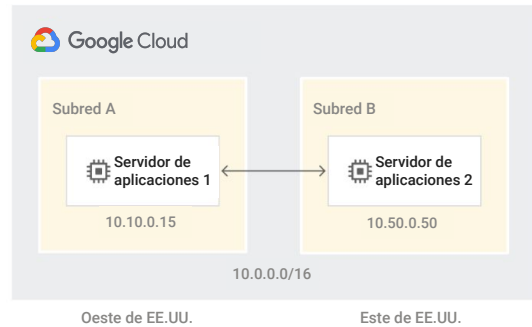
En Google Cloud, las redes de VPC son globales. Puede crear redes en modo automático, que tienen una subred por región, o bien crear su propia red en modo personalizado, que permite especificar la región donde se establecen las subredes.

Los recursos entre regiones pueden comunicarse usando sus direcciones IP internas sin ninguna interconexión adicional. Por ejemplo, en el diagrama de la derecha, se muestran dos subredes de distintas regiones con un servidor en cada una. Estas pueden comunicarse entre sí usando sus direcciones IP internas porque están conectadas a la misma red de VPC.

La selección de las regiones en las que creará subredes depende de sus requisitos. Por ejemplo, si forma parte de una empresa global, lo más probable es que cree subredes en varias regiones del mundo. Si los usuarios se encuentran en una región específica, sería más adecuado seleccionar solo una subred en la región más cercana para los usuarios y, quizás, establecer una región de respaldo. Además, puede tener varias redes por proyecto. Estas redes son solo un conjunto de subredes regionales.

En Google Cloud, las redes de VPC son globales

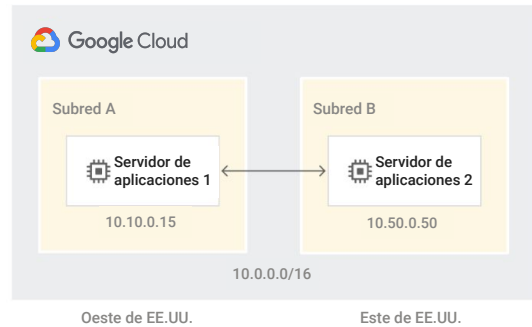
- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



En Google Cloud, las redes de VPC son globales...

En Google Cloud, las redes de VPC son globales

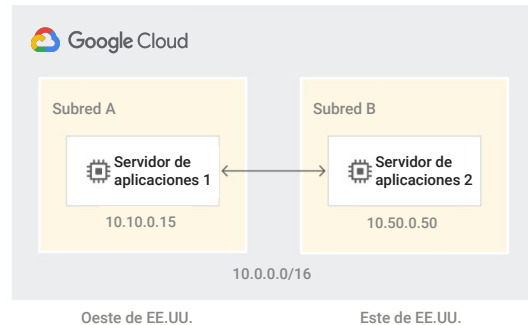
- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



y usted puede crear redes en modo automático, que tienen una subred por región, o bien crear una red en modo personalizado, que permite especificar la región donde se establecen las subredes.

En Google Cloud, las redes de VPC son globales

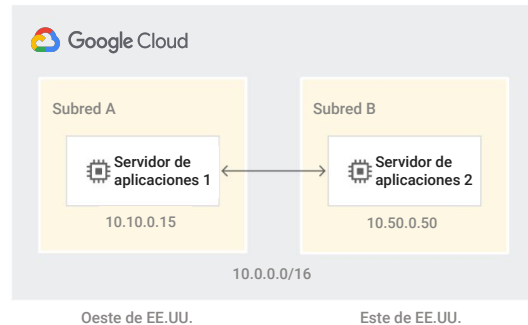
- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



Los recursos entre regiones pueden comunicarse usando sus direcciones IP internas sin ninguna interconexión adicional. Por ejemplo, en el diagrama de la derecha, se muestran dos subredes de distintas regiones con un servidor en cada una. Estas pueden comunicarse entre sí usando sus direcciones IP internas porque están conectadas a la misma red de VPC.

En Google Cloud, las redes de VPC son globales

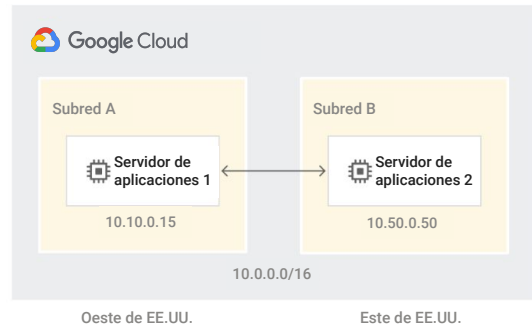
- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



La selección de las regiones en las que creará subredes depende de sus requisitos. Por ejemplo, si forma parte de una empresa global, lo más probable es que cree subredes en varias regiones del mundo.

En Google Cloud, las redes de VPC son globales

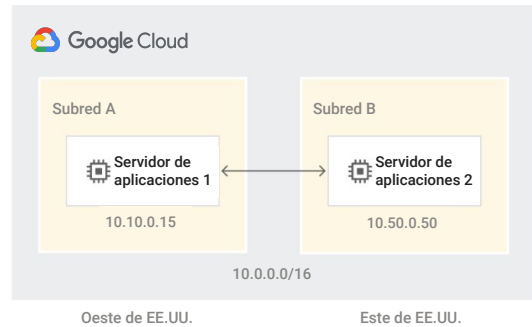
- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



Si los usuarios se encuentran en una región específica, sería más adecuado seleccionar solo una subred en la región más cercana para los usuarios y, quizás, establecer una región de respaldo.

En Google Cloud, las redes de VPC son globales

- Cuando cree redes, cree subredes para las regiones en las que desee operar.
- Los recursos entre regiones pueden comunicarse entre sí sin ninguna interconexión adicional.
- Si es miembro de una empresa global, elija regiones de todo el mundo.
- Si sus usuarios no están tan lejos unos de otros, elija la región más cercana para ellos y una región de respaldo.
- Un proyecto puede tener varias redes.



Además, puede tener varias redes por proyecto. Estas redes son solo un conjunto de subredes regionales.

Cuando cree subredes personalizadas, especifique la región y el rango de direcciones IP internas

- No se deben superponer los rangos de direcciones IP.
- Las máquinas de una misma VPC pueden comunicarse con sus direcciones IP internas, independientemente de la región de la subred.
- No es necesario derivar las subredes desde un solo bloque de CIDR.
- Se pueden expandir las subredes sin tiempo de inactividad.
- Se pueden configurar alias de IP o rangos secundarios en la subred.

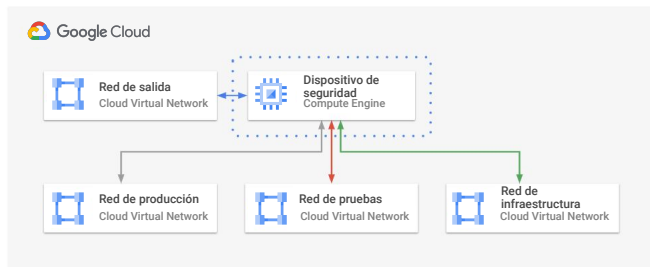
The image shows two overlapping screenshots of the AWS Management Console 'Nueva subred' (New Subnet) form. The top screenshot shows the 'Nombre' (Name) field with the value 'virginia' and the 'Región' (Region) dropdown menu set to 'us-east4'. The bottom screenshot shows the 'Nombre' field with the value 'iowa', the 'Región' dropdown set to 'us-central1', and the 'Rango de direcciones IP' (IP address range) field with the value '10.0.2.0/24'. Both screenshots show the 'Agregar una descripción' (Add description) link and the 'Crear rango de IP secundario' (Create secondary IP range) link.

Para crear subredes personalizadas, especifique la región y el rango de direcciones IP internas, como se muestra en las capturas de pantalla. No es necesario derivar los rangos de IP de estas subredes desde un solo bloque de CIDR, pero no pueden superponerse con otras subredes de la misma red de VPC. Esto se aplica a los rangos principales y a los secundarios. Los rangos secundarios le permiten definir direcciones IP de alias.

También puede expandir el espacio de direcciones IP principales de cualquier subred sin interrumpir las cargas de trabajo y sin tiempo de inactividad. Cuando defina las subredes, las máquinas de la misma red de VPC podrán comunicarse entre sí con sus direcciones IP internas, independientemente de la subred a la que estén conectadas.

Una sola VM puede tener varias interfaces de red conectadas a distintas redes.

- Cada red debe tener una subred en la región donde se creó la VM.
- Cada interfaz debe conectarse a una red de VPC distinta.
- Se admite un máximo de 8 interfaces por VM.



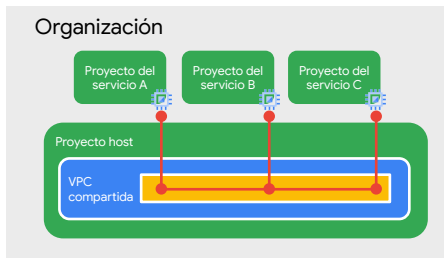
Una sola VM puede tener varias interfaces de red conectadas a distintas redes de VPC. En este gráfico, se ilustra un ejemplo de una instancia de Compute Engine conectada a cuatro redes distintas que abarcan la producción, las pruebas, la infraestructura y una red de salida.

Una VM debe contar con al menos una interfaz de red, pero puede tener hasta 8, lo que depende del tipo de instancia y la cantidad de CPU virtuales. Una regla general es que, con más CPU virtuales, se pueden tener más interfaces de red. Todas estas interfaces deben crearse junto con la instancia y cada una de ellas debe conectarse a una red distinta.

Una VPC compartida se crea en un solo proyecto, pero puede compartirse y usarse en otros

Se necesita una organización

- Cree la VPC en el proyecto host.
- El administrador de la VPC compartida la comparte con otros proyectos de servicios.



Brinda un control centralizado sobre la configuración de red

- Los administradores de red configuran subredes, reglas de firewall, rutas, etcétera.
- Quita a los desarrolladores los derechos de administrador de la red.
- Los desarrolladores se enfocan en crear y configurar máquinas en la red compartida.
- Inhabilita la creación de la red predeterminada con una política de la organización.

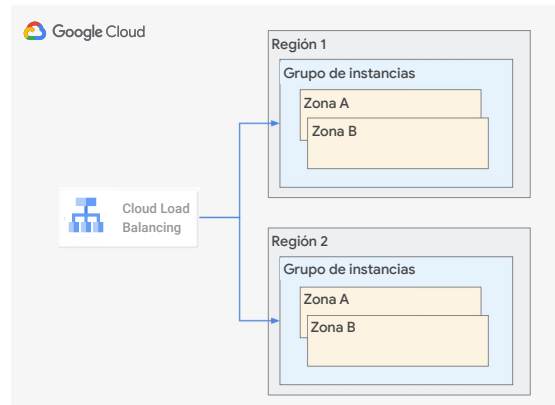
La VPC compartida permite que una organización conecte sus recursos desde varios proyectos a una red de VPC común. De esta forma, los recursos se pueden comunicar entre sí de forma segura y eficiente mediante IP internas de esa red.

En este gráfico, se muestra una situación en la que tres proyectos de servicios (A, B y C) usan una VPC compartida. Cada uno de ellos tiene una instancia de VM conectada a esa red.

La VPC compartida brinda un enfoque centralizado de redes de varios proyectos, dado que las políticas de red y seguridad tienen lugar en una sola red de VPC designada. Esto permite quitar los derechos de administrador de red a los desarrolladores para que se enfoquen en lo que hacen mejor. Al mismo tiempo, los administradores de red de la organización mantienen el control sobre los recursos, como las subredes, las reglas de firewall y las rutas, y delegan el control de crear recursos, como las instancias, a los administradores o desarrolladores de proyectos de servicios.

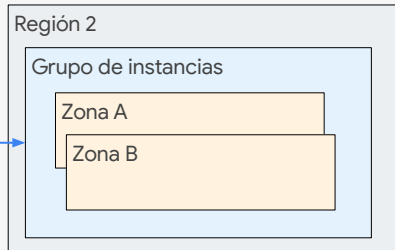
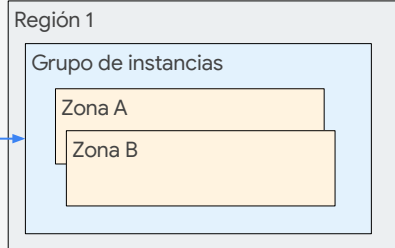
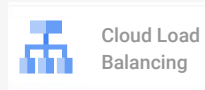
Use un balanceador de cargas global para proporcionar acceso a servicios implementados en varias regiones.

- El balanceo de cargas global es compatible con balanceadores de cargas HTTP y proxies TCP y SSL.
- El balanceador de cargas HTTP enruta las solicitudes a las regiones que están más cerca del usuario.
 - Usa una dirección IP Anycast global.



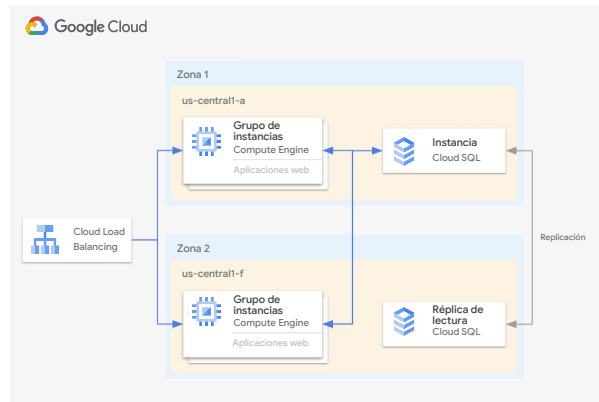
Hablemos sobre los balanceadores de cargas. Los balanceadores de cargas globales proporcionan acceso a servicios implementados en varias regiones. Por ejemplo, el que se muestra en esta diapositiva tiene un backend con dos grupos de instancias implementados en distintas regiones. Cloud Load Balancing se usa para distribuir la carga entre estos grupos de instancias.

El balanceo de cargas global es compatible con los balanceadores HTTP y con proxies TCP y SSL en Google Cloud. Para un balanceador de cargas HTTP, se puede usar una dirección IP Anycast global, lo que simplifica la búsqueda de DNS. De forma predeterminada, las solicitudes se enrutan a la región que está más cerca del solicitante.



Use un balanceador de cargas regional para proporcionar acceso a los servicios implementados en una sola región

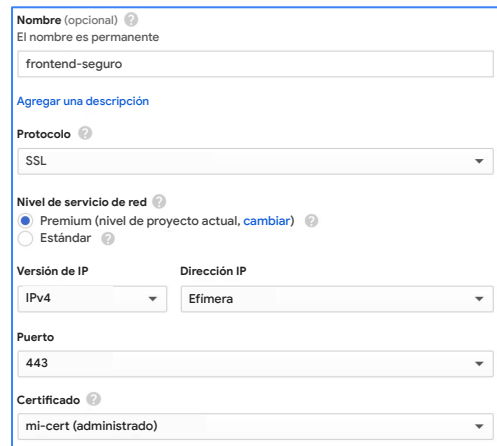
- Es compatible con balanceadores de cargas HTTP, TCP y UDP.
- Puede tener una dirección IP pública o privada.
- Puede usar cualquier puerto TCP o UDP.



Para los servicios implementados en una sola región, use un balanceador de cargas regional. En este gráfico, se ilustran los recursos implementados en una sola región y las solicitudes de enrutamiento de Cloud Load Balancing para esos recursos. Los balanceadores de cargas regionales son compatibles con HTTP(S) y cualquier puerto TCP o UDP.

Si sus balanceadores de cargas tienen IP públicas, protéjalas con SSL

- Es compatible con balanceadores de cargas HTTP y TCP.
- Cuenta con certificados SSL autoadministrados y administrados por Google.



Nombre (opcional) ⓘ
El nombre es permanente
frontend-seguro

[Agregar una descripción](#)

Protocolo ⓘ
SSL

Nivel de servicio de red ⓘ
☒ Premium (nivel de proyecto actual, [cambiar](#)) ⓘ
☐ Estándar ⓘ

Versión de IP Dirección IP
IPv4 Efímera

Puerto
443

Certificado ⓘ
mi-cert (administrado)

Si sus balanceadores de cargas tienen direcciones IP públicas, el tráfico seguramente transitará por Internet. Recomendando que proteja este tráfico con SSL, que está disponible para balanceadores de cargas HTTP y TCP, como se muestra en la captura de pantalla de la derecha.

Puede usar certificados SSL autoadministrados o administrados por Google cuando utilice esta tecnología.

Aproveche Cloud CDN para reducir la latencia y el costo de salida

- Se puede habilitar cuando se configura el balanceador de cargas HTTP global.
- Almacena en caché el contenido de forma global usando las ubicaciones de almacenamiento en caché perimetral de Google Cloud.
- Almacena en caché datos estáticos de servidores web, en instancias de Compute Engine, Pods de GKE o buckets de Cloud Storage.



Si usa balanceo de cargas HTTP(S), debería aprovechar Cloud CDN para reducir la latencia y los costos de salida. Puede habilitarlo marcando la casilla de verificación correspondiente cuando configure un balanceador de cargas HTTP(S) global. Cloud CDN almacena contenido en caché de forma global usando las ubicaciones de almacenamiento en caché perimetral de Google Cloud, por lo que el contenido se almacena en caché más cerca de los usuarios que realizan solicitudes.

Los datos que se almacenan en caché pueden provenir de una variedad de fuentes, como instancias de Compute Engine, Pods de GKE o buckets de Cloud Storage.

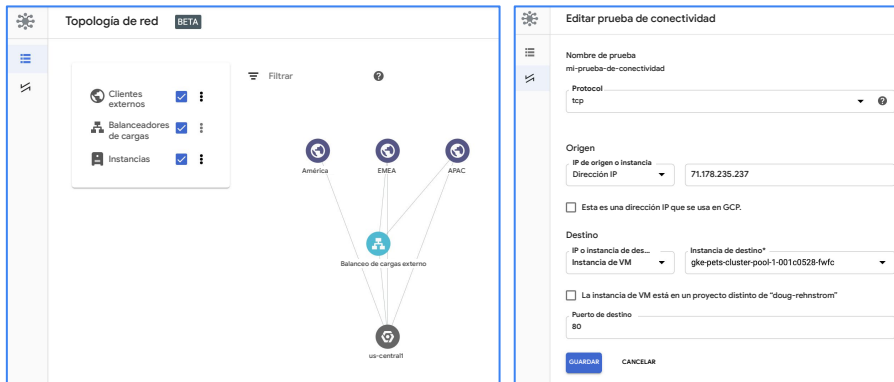
Tipos de balanceadores de cargas de Google Cloud y sus funciones

Balanceo de cargas de HTTP(S)	Balanceo de cargas de TCP	Balanceo de cargas UDP
Balanceo de cargas de capa 7 para aplicaciones HTTP y HTTPS Más información	Balanceo de cargas de capa 4 o proxy para aplicaciones que dependen del protocolo TCP/SSL Más información	Balanceo de cargas de capa 4 para aplicaciones que dependen del protocolo UDP Más información
Configurar LB de HTTP LB de HTTPS (incluye LB de HTTP/2)	Configurar LB de TCP Proxy SSL Proxy TCP	Configurar LB de UDP
Opciones Orientado a Internet o interno Para una o varias regiones	Opciones Orientado a Internet o Para una o varias regiones	Opciones Orientado a Internet o interno Una sola región
Iniciar configuración	Iniciar configuración	Iniciar configuración

Ahora presentaré una síntesis sobre los balanceadores de cargas de Google Cloud y sus funciones. En general, los balanceadores de cargas pueden funcionar con direcciones IP internas o externas. Las externas se consideran *orientadas a Internet*. Los balanceadores de cargas pueden ser regionales o multirregionales, y admiten distintos tipos de tráfico, como HTTP, TCP y UDP. Revisemos estos tipos de balanceo de cargas, comenzando por el tipo de tráfico.

- El balanceo de cargas HTTP(S) consiste en un balanceador de cargas de capa 7. Es compatible con HTTP y HTTPS, incluido HTTP/2. Además, admite el balanceo de cargas interno y orientado a Internet, así como el regional o el global.
- El balanceo de cargas de TCP proporciona balanceo de capa 4 o proxy para aplicaciones que requieren el protocolo TCP/SSL. Puede configurar un balanceador de cargas TCP o un proxy TCP o SSL. Además, admite el balanceo de cargas interno y orientado a Internet, así como el regional y el global.
- El balanceo de cargas de UDP es para aquellas aplicaciones que dependen del protocolo UDP. Admite el balanceo de cargas interno y orientado a Internet, pero solo el tráfico regional.

Network Intelligence Center se puede usar para visualizar la topología de red y probar la conectividad de red



Como parte de nuestra conversación sobre el diseño de redes de VPC, también quiero mencionar Network Intelligence Center, un servicio de Google Cloud que puede utilizarse para visualizar la topología de sus redes de VPC y probar la conectividad de red.

En el gráfico de la izquierda, se muestra una visualización de topología de red sencilla con clientes externos en tres regiones y un tráfico que se enruta por un balanceador de cargas externo a los recursos de us-central1. Esta facilidad de uso es extremadamente valiosa para confirmar la topología de red cuando se configura una red o cuando se realizan diagnósticos. En el gráfico de la derecha, se muestra la configuración de una prueba de conectividad entre un origen y un destino junto con un protocolo y un puerto. Se pueden realizar las siguientes pruebas:

- Entre los extremos de origen y destino en su red de Nube privada virtual (VPC)
- Desde su red de VPC, desde y hacia Internet
- Desde su red de VPC, desde y hacia su red local

Actividad 8: Defina las características de la red

Consulte el cuaderno de ejercicios de Design and Process.

- Especifique las características de la red de VPC del caso de éxito.
- Seleccione el tipo de balanceador de cargas que se requiere para cada servicio.



En esta actividad de diseño, debe especificar las características de la red del caso de éxito y seleccionar el tipo de balanceador de cargas que se requiere para cada servicio.

Actividad 8: Defina las características de la red

Consulte el cuaderno de ejercicios de Design and Process.

- Especifique las características de la red de VPC del caso de éxito.
- Seleccione el tipo de balanceador de cargas que se requiere para cada servicio.



En esta actividad de diseño...

Actividad 8: Defina las características de la red

Consulte el cuaderno de ejercicios de Design and Process.

- Especifique las características de la red de VPC del caso de éxito.
- Seleccione el tipo de balanceador de cargas que se requiere para cada servicio.



debe especificar las características de la red del caso de éxito y...

Actividad 8: Defina las características de la red

Consulte el cuaderno de ejercicios de Design and Process.

- Especifique las características de la red de VPC del caso de éxito.
- Seleccione el tipo de balanceador de cargas que se requiere para cada servicio.



seleccionar el tipo de balanceador de cargas que se requiere para cada servicio.

Servicio	Orientado a Internet o solo para uso interno	HTTP	TCP	UDP	Multirregional
Cuentas	Solo para uso interno		Sí		No

En esta primera parte de la actividad, complete esta tabla para describir las características de la red de cada uno de sus servicios.

El ejemplo que se muestra aquí corresponde al servicio de cuentas. Como se trata de un servicio de backend, solo se puede acceder a él de manera interna con TCP, y no pretendemos implementarlo en varias regiones.

Servicio	HTTP	TCP	UDP
Cuentas		X	

Luego, en función de las características de red de cada servicio, use esta tabla para seleccionar el balanceador de cargas correcto. Según los parámetros de la diapositiva anterior, usaremos el balanceador de cargas TCP regional.

Consulte las actividades 8a y 8b en el cuaderno de ejercicios de diseño a fin de completar tablas similares para otros servicios y explore Cloud CDN para reducir la latencia y los costos de salida de red.

Revisión de la actividad 8: Defina las características de la red

- Especifique las características de la red de VPC del caso de éxito.
- Seleccione el tipo de balanceador de cargas que se requiere para cada servicio.






En esta actividad, se le pidió especificar las características de la red de cada uno de sus servicios y seleccionar el balanceador de cargas adecuado para cada uno de ellos.

Servicio	Orientado a Internet o solo para uso interno	HTTP	TCP	UDP	Multirregional
Búsqueda	Orientado a Internet	X			Sí
Inventario	Interno		X		No
Análisis	Orientado a Internet	X			No
IU web	Orientado a Internet	X			Sí
Pedidos	Interno		X		No

Este es un ejemplo completo de TurisClic, nuestro portal de viajes en línea.

Los servicios de inventario y pedidos son internos y regionales, y usan TCP. Los demás servicios se deben orientar a Internet mediante HTTP. Decidimos implementar estos servicios en múltiples regiones a fin de obtener una latencia más baja, un mejor rendimiento y una alta disponibilidad para los usuarios que se encuentran en otros países del mundo.

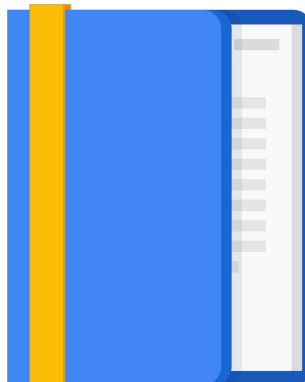
Servicio	 HTTP	 TCP	 UDP
Búsqueda	X		
Inventario		X	
Análisis	X		
IU web	X		
Pedidos		X	

Según las características de esas redes, elegimos el balanceador de cargas HTTP global para los servicios orientados al público y el balanceador de cargas TCP interno para los servicios orientados al sistema interno.

Temario

Diseñe redes de
Google Cloud

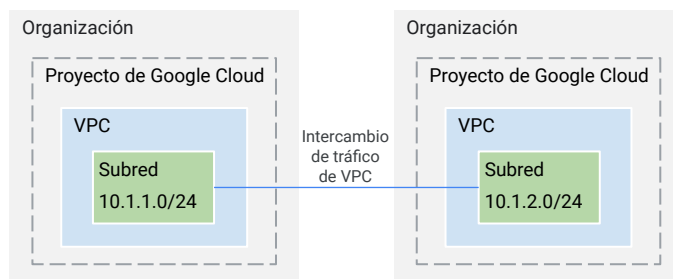
Conecte redes



Enfoquémonos en los productos de conectividad de red de Google Cloud, que son el intercambio de tráfico, Cloud VPN y Cloud Interconnect.

Use el intercambio de tráfico de VPC para conectar redes cuando ambas se encuentran en Google Cloud

- Puede ser dentro de la misma organización o entre organizaciones distintas.
- No se deben superponer los rangos de subredes.
- Los administradores de red de cada VPC deben aprobar las solicitudes de intercambio de tráfico.



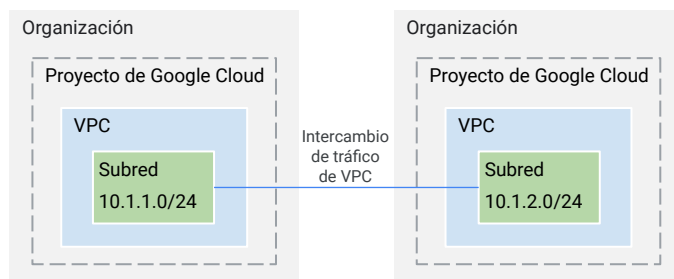
Google Cloud

Si intenta conectar dos redes de VPC, debería considerar el intercambio de tráfico de VPC, que permite la conectividad privada RFC 1918 entre dos redes de VPC, independientemente de si pertenecen al mismo proyecto o a la misma organización. Recuerde que cada red de VPC tendrá reglas de firewall que definen el tráfico que se permite o rechaza entre las redes.

En este diagrama, se muestra una conexión de intercambio de tráfico de VPC entre dos redes que pertenecen a distintos proyectos y organizaciones. Seguramente note que los rangos de subredes no se superponen. Este es uno de los requisitos para establecer una conexión. Además, los administradores de cada red de VPC deben configurar la solicitud de intercambio de tráfico correspondiente para establecer la conexión.

Use el intercambio de tráfico de VPC para conectar redes cuando ambas se encuentran en Google Cloud

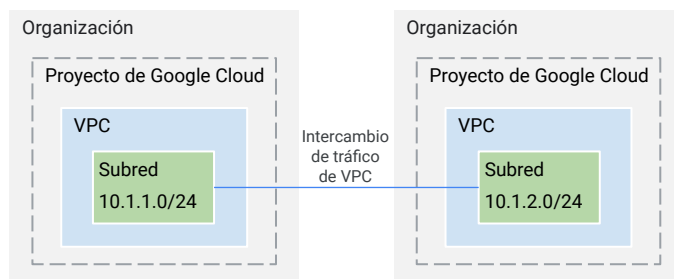
- Puede ser dentro de la misma organización o entre organizaciones distintas.
- No se deben superponer los rangos de subredes.
- Los administradores de red de cada VPC deben aprobar las solicitudes de intercambio de tráfico.



Si intenta conectar dos redes de VPC, debería considerar el intercambio de tráfico de VPC...

Use el intercambio de tráfico de VPC para conectar redes cuando ambas se encuentran en Google Cloud

- Puede ser dentro de la misma organización o entre organizaciones distintas.
- No se deben superponer los rangos de subredes.
- Los administradores de red de cada VPC deben aprobar las solicitudes de intercambio de tráfico.

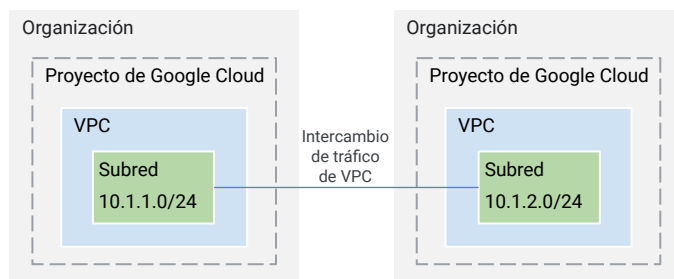


que permite la conectividad privada RFC 1918 entre dos redes de VPC, independientemente de si pertenecen al mismo proyecto o a la misma organización. Recuerde que cada red de VPC tendrá reglas de firewall que definen el tráfico que se permite o rechaza entre las redes.

En este diagrama, se muestra una conexión de intercambio de tráfico de VPC entre dos redes que pertenecen a distintos proyectos y organizaciones.

Use el intercambio de tráfico de VPC para conectar redes cuando ambas se encuentran en Google Cloud

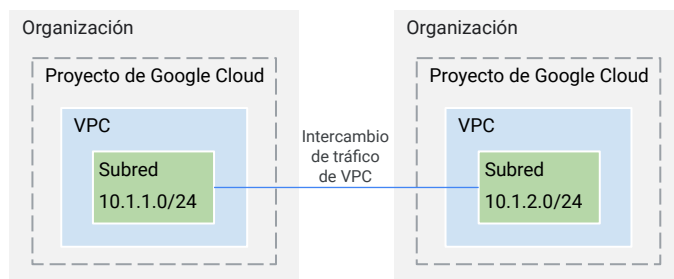
- Puede ser dentro de la misma organización o entre organizaciones distintas.
- No se deben superponer los rangos de subredes.
- Los administradores de red de cada VPC deben aprobar las solicitudes de intercambio de tráfico.



Seguramente note que los rangos de subredes no se superponen. Este es uno de los requisitos para establecer una conexión.

Use el intercambio de tráfico de VPC para conectar redes cuando ambas se encuentran en Google Cloud

- Puede ser dentro de la misma organización o entre organizaciones distintas.
- No se deben superponer los rangos de subredes.
- Los administradores de red de cada VPC deben aprobar las solicitudes de intercambio de tráfico.



Además, los administradores de cada red de VPC deben configurar la solicitud de intercambio de tráfico correspondiente para establecer la conexión.

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud

- Útil para conexiones de datos de bajo volumen
- VPN clásica: ANS del 99.9%
- VPN con alta disponibilidad: ANS del 99.99%
- Admite:
 - VPN de sitio a sitio
 - Rutas estáticas (solo para VPN clásicas)
 - Rutas dinámicas (Cloud Router)
 - Algoritmos de cifrado IKEv1 e IKEv2



Cloud VPN

Google Cloud

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud mediante un túnel VPN con IPsec. Una puerta de enlace VPN encripta el tráfico que viaja entre las dos redes, el que, luego, es desencriptado por la otra puerta de enlace VPN. De esta forma, se protegen sus datos mientras viajan por Internet pública. Es por este motivo que Cloud VPN resulta útil para las conexiones de datos de bajo volumen.

Como servicio administrado, Cloud VPN proporciona un ANS del 99.9% de tiempo de actividad mensual para la configuración de VPN clásicas, y un tiempo de actividad mensual del 99.99% para la configuración de VPN con alta disponibilidad. Las puertas de enlace de VPN clásicas tienen solo una interfaz y una dirección IP externa. En cambio, las puertas de enlace de las VPN con alta disponibilidad tienen dos interfaces con dos direcciones IP externas (una para cada puerta de enlace). La elección de la puerta de enlace de VPN depende del ANS que necesite y las opciones de enrutamiento.

Cloud VPN admite VPN de sitio a sitio y rutas estáticas y dinámicas con Cloud Router y algoritmos de cifrado IKEv1 e IKEv2. Sin embargo, solo las VPN clásicas son compatibles con las rutas estáticas.

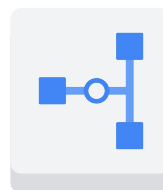
Además, Cloud VPN no es compatible con los casos de uso en los que las

computadoras clientes deban “conectarse” a una VPN mediante software cliente.

Para obtener más información sobre el ANS y estas funciones, consulte la documentación: <https://cloud.google.com/vpn/docs/concepts/overview>

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud

- Útil para conexiones de datos de bajo volumen
- VPN clásica: ANS del 99.9%
- VPN con alta disponibilidad: ANS del 99.99%
- Admite:
 - VPN de sitio a sitio
 - Rutas estáticas (solo para VPN clásicas)
 - Rutas dinámicas (Cloud Router)
 - Algoritmos de cifrado IKEv1 e IKEv2

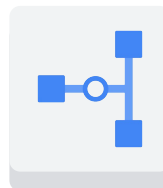


Cloud VPN

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud mediante un túnel VPN con IPsec. Una puerta de enlace VPN encripta el tráfico que viaja entre las dos redes, el que, luego, es descifrado por la otra puerta de enlace VPN. De esta forma, se protegen sus datos mientras viajan por Internet pública. Es por este motivo que Cloud VPN resulta útil para las conexiones de datos de bajo volumen.

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud

- Útil para conexiones de datos de bajo volumen
- VPN clásica: [ANS del 99.9%](#)
- VPN con alta disponibilidad: ANS del 99.99%
- Admite:
 - VPN de sitio a sitio
 - Rutas estáticas (solo para VPN clásicas)
 - Rutas dinámicas (Cloud Router)
 - Algoritmos de cifrado IKEv1 e IKEv2

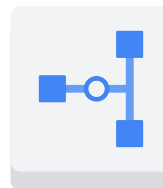


Cloud VPN

Como servicio administrado, Cloud VPN proporciona un ANS del 99.9% de tiempo de actividad mensual para la configuración de VPN clásica.

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud

- Útil para conexiones de datos de bajo volumen
- VPN clásica: ANS del 99.9%
- **VPN con alta disponibilidad: ANS del 99.99%**
- Admite:
 - VPN de sitio a sitio
 - Rutas estáticas (solo para VPN clásicas)
 - Rutas dinámicas (Cloud Router)
 - Algoritmos de cifrado IKEv1 e IKEv2

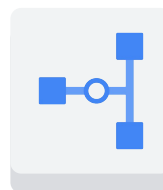


Cloud VPN

Y un tiempo de actividad mensual del 99.99% para la configuración de VPN con alta disponibilidad. Las puertas de enlace de VPN clásicas tienen solo una interfaz y una dirección IP externa. En cambio, las puertas de enlace de las VPN con alta disponibilidad tienen dos interfaces con dos direcciones IP externas (una para cada puerta de enlace). La elección de la puerta de enlace de VPN depende del ANS que necesite y las opciones de enrutamiento.

Cloud VPN conecta de manera segura su red local a la red de VPC de Google Cloud

- Útil para conexiones de datos de bajo volumen
- VPN clásica: ANS del 99.9%
- VPN con alta disponibilidad: ANS del 99.99%
- **Admite:**
 - VPN de sitio a sitio
 - Rutas estáticas (solo para VPN clásicas)
 - Rutas dinámicas (Cloud Router)
 - Algoritmos de cifrado IKEv1 e IKEv2



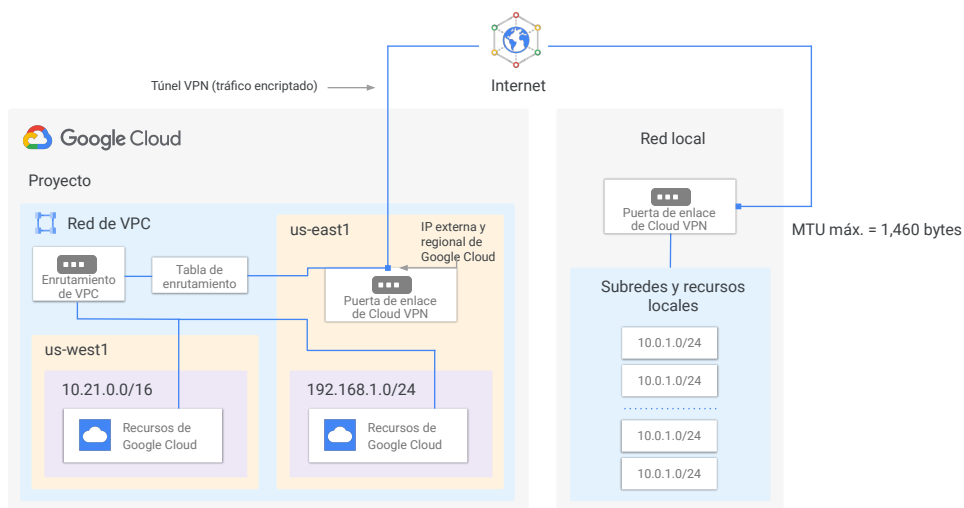
Cloud VPN

Cloud VPN admite VPN de sitio a sitio y rutas estáticas y dinámicas con Cloud Router y algoritmos de cifrado IKEv1 e IKEv2. Sin embargo, solo las VPN clásicas son compatibles con las rutas estáticas.

Además, Cloud VPN no es compatible con los casos de uso en los que las computadoras clientes deban “conectarse” a una VPN mediante software cliente.

Para obtener más información sobre el ANS y estas funciones, consulte la documentación: <https://cloud.google.com/vpn/docs/concepts/overview>

Topología de VPN clásica



Google Cloud

Explicaré un ejemplo de Cloud VPN. En este diagrama, se muestra una conexión de VPN clásica entre su red de VPC y la red local. La de VPC tiene subredes en us-east1 y us-west1, así como recursos de Google Cloud en cada una de esas regiones.

Estos recursos se pueden comunicar mediante su dirección IP interna porque el enrutamiento dentro de una red se configura automáticamente (si se supone que las reglas de firewall permiten la comunicación).

Ahora, para conectar la red local y sus recursos, debe configurar su puerta de enlace de Cloud VPN, la puerta de enlace de VPN local y dos túneles VPN. La puerta de enlace de Cloud VPN es un recurso regional que usa una dirección IP externa regional.

La puerta de enlace de VPN local puede ser un dispositivo físico de su centro de datos o una oferta de VPN física o basada en software en la red de otro proveedor de servicios en la nube. Esta puerta de enlace de VPN también tiene una dirección IP externa.

Luego, un túnel VPN conecta las puertas de enlace de VPN y funciona como el medio virtual por el que pasa el tráfico encriptado. Para crear una conexión entre dos

puertas de enlace de VPN, debe establecer dos túneles VPN. Cada túnel define la conexión desde la perspectiva de su puerta de enlace, en la que el tráfico solo puede pasar cuando se establece el par de túneles.

Cuando utilice Cloud VPN, no olvide que la unidad de transmisión máxima (MTU) para su puerta de enlace de VPN local no puede ser mayor que 1,460 bytes. Esto se debe a la encriptación y el encapsulamiento de paquetes. Para obtener más información sobre esta consideración de MTU consulte la documentación:

<https://cloud.google.com/vpn/docs/concepts/mtu-considerations>.

Además de la VPN clásica, Google Cloud también ofrece un segundo tipo de puerta de enlace de Cloud VPN, llamada VPN con alta disponibilidad.

Descripción general de la VPN con alta disponibilidad

- Proporciona una disponibilidad del servicio del 99.99%.
- Google Cloud elige de forma automática dos direcciones IP externas.
 - Admite varios túneles.
 - Los túneles VPN conectados a las puertas de enlace de VPN con alta disponibilidad deben usar el enrutamiento dinámico (BGP).
- Admite VPN de sitio a sitio para distintas situaciones de topología y configuración:
 - Una puerta de enlace de VPN con alta disponibilidad para intercambiar tráfico entre dispositivos VPN
 - Una puerta de enlace de VPN con alta disponibilidad conectada a una puerta de enlace virtual de Amazon Web Services (AWS)
 - Dos puertas de enlace de VPN con alta disponibilidad conectadas entre sí

Google Cloud

Se trata de una solución de Cloud VPN con alta disponibilidad que le permite conectar de forma segura su red local a la red de nube privada virtual (VPC) mediante una conexión de VPN con IPsec en una sola región. Ofrece un ANS del 99.99% de disponibilidad del servicio. A fin de garantizar un ANS del 99.99% de disponibilidad para las conexiones VPN con alta disponibilidad, debe configurar dos o cuatro túneles de forma correcta desde su puerta de enlace de VPN con alta disponibilidad a su puerta de enlace de VPN de intercambio de tráfico o a otra puerta de enlace de VPN con alta disponibilidad.

Cuando crea una puerta de enlace de VPN con alta disponibilidad, Google Cloud elige de forma automática dos direcciones IP externas, una para cada una de las dos interfaces fijas. Cada dirección IP se elige de forma automática a partir de un grupo de direcciones único para admitir la alta disponibilidad.

Cada una de las interfaces de puerta de enlace de VPN con alta disponibilidad admite varios túneles. También puede crear varias puertas de enlace de VPN con alta disponibilidad. Cuando borra la puerta de enlace de VPN con alta disponibilidad, Google Cloud libera las direcciones IP para que puedan volver a usarse. Puede configurar una puerta de enlace de VPN con alta disponibilidad con una sola interfaz activa y una dirección IP externa. Sin embargo, esta configuración no proporciona un ANS del 99.99% de disponibilidad del servicio. Los túneles VPN conectados a las puertas de enlace de VPN con alta disponibilidad deben usar el enrutamiento dinámico (BGP). Según el método de configuración de las prioridades de ruta para los túneles VPN con alta disponibilidad, puede crear una configuración de

enrutamiento activa/activa o activa/pasiva.

La VPN con alta disponibilidad es compatible con VPN de sitio a sitio en una de las siguientes topologías o situaciones de configuración recomendadas:

- Una puerta de enlace de VPN con alta disponibilidad para intercambiar tráfico entre dispositivos VPN
- Una puerta de enlace de VPN con alta disponibilidad conectada a una puerta de enlace virtual de Amazon Web Services (AWS)
- Dos puertas de enlace de VPN con alta disponibilidad conectadas entre sí

Exploremos estos parámetros de configuración con más detalle.

Descripción general de la VPN con alta disponibilidad

- Proporciona una disponibilidad del servicio del 99.99%.
- Google Cloud elige de forma automática dos direcciones IP externas.
 - Admite varios túneles.
 - Los túneles VPN conectados a las puertas de enlace de VPN con alta disponibilidad deben usar el enrutamiento dinámico (BGP).
- Admite VPN de sitio a sitio para distintas situaciones de topología y configuración:
 - Una puerta de enlace de VPN con alta disponibilidad para intercambiar tráfico entre dispositivos VPN
 - Una puerta de enlace de VPN con alta disponibilidad conectada a una puerta de enlace virtual de Amazon Web Services (AWS)
 - Dos puertas de enlace de VPN con alta disponibilidad conectadas entre sí

Google Cloud

Se trata de una solución de Cloud VPN con alta disponibilidad que le permite conectar de forma segura su red local a la red de nube privada virtual (VPC) mediante una conexión de VPN con IPsec en una sola región. Ofrece un ANS del 99.99% de disponibilidad del servicio. A fin de garantizar un ANS del 99.99% de disponibilidad para las conexiones VPN con alta disponibilidad, debe configurar dos o cuatro túneles de forma correcta desde su puerta de enlace de VPN con alta disponibilidad a su puerta de enlace de VPN de intercambio de tráfico o a otra puerta de enlace de VPN con alta disponibilidad.

Descripción general de la VPN con alta disponibilidad

- Proporciona una disponibilidad del servicio del 99.99%.
- Google Cloud elige de forma automática dos direcciones IP externas.
 - Admite varios túneles.
 - Los túneles VPN conectados a las puertas de enlace de VPN con alta disponibilidad deben usar el enrutamiento dinámico (BGP).
- Admite VPN de sitio a sitio para distintas situaciones de topología y configuración:
 - Una puerta de enlace de VPN con alta disponibilidad para intercambiar tráfico entre dispositivos VPN
 - Una puerta de enlace de VPN con alta disponibilidad conectada a una puerta de enlace virtual de Amazon Web Services (AWS)
 - Dos puertas de enlace de VPN con alta disponibilidad conectadas entre sí

Google Cloud

Cuando crea una puerta de enlace de VPN con alta disponibilidad, Google Cloud elige de forma automática dos direcciones IP externas, una para cada una de las dos interfaces fijas. Cada dirección IP se elige de forma automática a partir de un grupo de direcciones único para admitir la alta disponibilidad.

Cada una de las interfaces de puerta de enlace de VPN con alta disponibilidad admite varios túneles. También puede crear varias puertas de enlace de VPN con alta disponibilidad. Cuando borra la puerta de enlace de VPN con alta disponibilidad, Google Cloud libera las direcciones IP para que puedan volver a usarse. Puede configurar una puerta de enlace de VPN con alta disponibilidad con una sola interfaz activa y una dirección IP externa. Sin embargo, esta configuración no proporciona un ANS del 99.99% de disponibilidad del servicio. Los túneles VPN conectados a las puertas de enlace de VPN con alta disponibilidad deben usar el enrutamiento dinámico (BGP). Según el método de configuración de las prioridades de ruta para los túneles VPN con alta disponibilidad, puede crear una configuración de enrutamiento activa/activa o activa/pasiva.

Descripción general de la VPN con alta disponibilidad

- Proporciona una disponibilidad del servicio del 99.99%.
- Google Cloud elige de forma automática dos direcciones IP externas.
 - Admite varios túneles.
 - Los túneles VPN conectados a las puertas de enlace de VPN con alta disponibilidad deben usar el enrutamiento dinámico (BGP).
- Admite VPN de sitio a sitio para distintas situaciones de topología y configuración:
 - Una puerta de enlace de VPN con alta disponibilidad para intercambiar tráfico entre dispositivos VPN
 - Una puerta de enlace de VPN con alta disponibilidad conectada a una puerta de enlace virtual de Amazon Web Services (AWS)
 - Dos puertas de enlace de VPN con alta disponibilidad conectadas entre sí

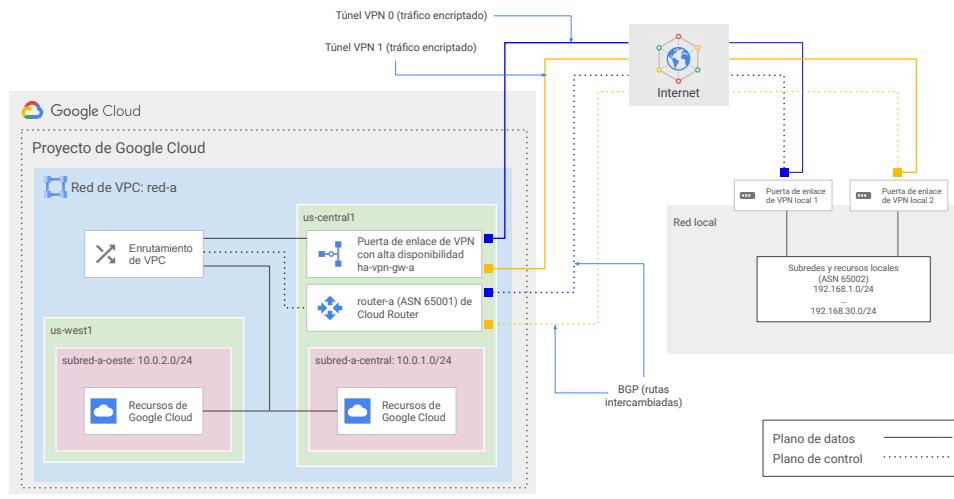
Google Cloud

La VPN con alta disponibilidad es compatible con VPN de sitio a sitio en una de las siguientes topologías o situaciones de configuración recomendadas:

- Una puerta de enlace de VPN con alta disponibilidad para intercambiar tráfico entre dispositivos VPN
- Una puerta de enlace de VPN con alta disponibilidad conectada a una puerta de enlace virtual de Amazon Web Services (AWS)
- Dos puertas de enlace de VPN con alta disponibilidad conectadas entre sí

Exploremos estos parámetros de configuración con más detalle.

Topología de VPN con alta disponibilidad para conectarse a puertas de enlace de VPN de intercambio de tráfico



Google Cloud

Existen tres opciones de configuración típicas de puerta de enlace de intercambio de tráfico para VPN con alta disponibilidad: 1) una puerta de enlace de VPN con alta disponibilidad a dos dispositivos VPN de intercambio de tráfico independientes, cada uno con su propia dirección IP; 2) una puerta de enlace de VPN con alta disponibilidad a un dispositivo VPN de intercambio de tráfico que usa dos direcciones IP distintas, y 3) una puerta de enlace de VPN con alta disponibilidad a un dispositivo VPN de intercambio de tráfico que usa solo una dirección IP.

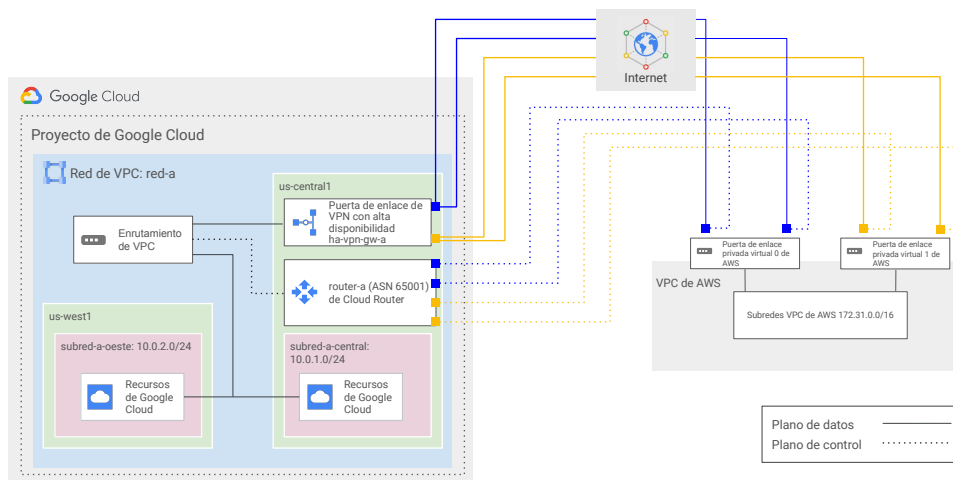
Veamos un ejemplo. En esta topología, una puerta de enlace de VPN con alta disponibilidad se conecta a dos dispositivos de intercambio de tráfico. Cada dispositivo de intercambio de tráfico tiene una interfaz y una dirección IP externa. La puerta de enlace de VPN con alta disponibilidad usa dos túneles, uno para cada dispositivo de intercambio de tráfico. Si su puerta de enlace de intercambio de tráfico está basada en hardware, tener una segunda proporciona redundancia y conmutación por error en ese lado de la conexión.

Una segunda puerta de enlace física le permite tomar una de las puertas de enlace sin conexión para actualizaciones de software o demás tareas de mantenimiento programadas. También lo protege si hay una falla en uno de los dispositivos.

En Google Cloud, el REDUNDANCY_TYPE de esta configuración toma el valor

TWO_IPS_REDUNDANCY. En este ejemplo, se proporciona una disponibilidad del 99.99%.

Topología de VPN con alta disponibilidad a una puerta de enlace de intercambio de tráfico de AWS

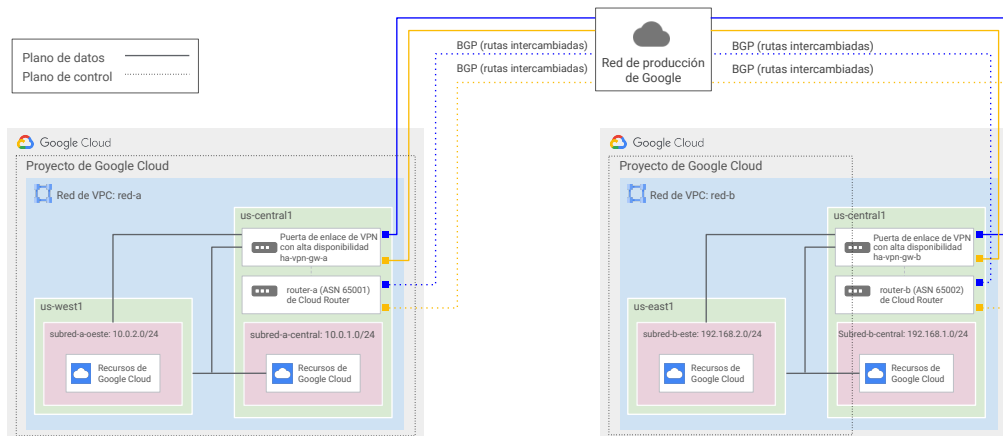


Google Cloud

Cuando configura una puerta de enlace de VPN externa de VPN con alta disponibilidad en Amazon Web Services (AWS), puede usar una puerta de enlace de tránsito o una puerta de enlace privada virtual. Solo la puerta de enlace de tránsito admite el enrutamiento de ruta múltiple de igual costo (ECMP). Cuando está habilitado, el ECMP distribuye de igual manera el tráfico entre los túneles activos. Veamos un ejemplo.

En esta topología, se deben configurar tres componentes principales de puertas de enlace: 1) una puerta de enlace de VPN con alta disponibilidad en Google Cloud con dos interfaces; 2) dos puertas de enlace privadas virtuales de AWS que conecten su puerta de VPN con alta disponibilidad, y 3) un recurso de puerta de enlace de VPN externa en Google Cloud que represente su puerta de enlace privada virtual de AWS. Este recurso proporciona a Google Cloud información sobre su puerta de enlace de AWS. La configuración admitida de AWS usa un total de cuatro túneles: dos de una puerta de enlace privada virtual de AWS para una interfaz de la puerta de VPN con alta disponibilidad y dos túneles de la otra puerta de AWS para la otra interfaz.

Topología de VPN con alta disponibilidad para conectarse a puertas de enlace de VPN de intercambio de tráfico

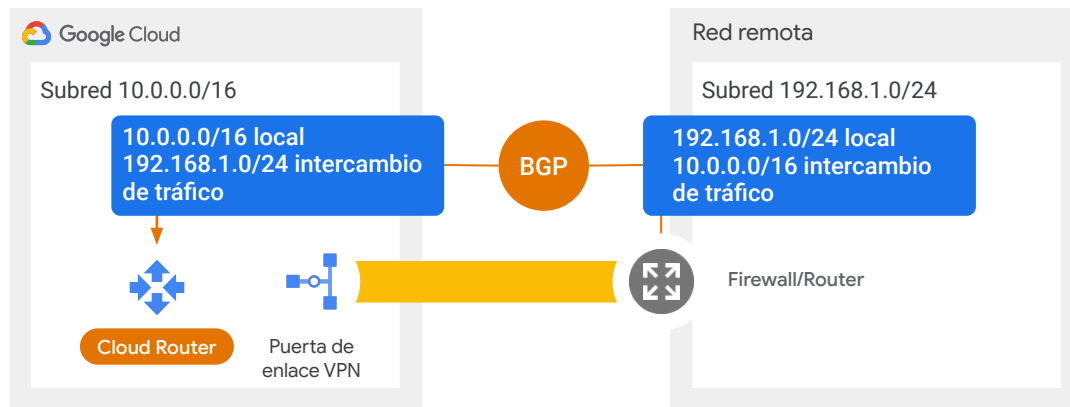


Google Cloud

Puede conectar dos redes de VPC de Google Cloud mediante una puerta de enlace de VPN con alta disponibilidad en cada red. La configuración que se muestra proporciona una disponibilidad del 99.99%. Desde la perspectiva de cada puerta de enlace de VPN con alta disponibilidad, usted crea dos túneles. Debe conectar la interfaz 0 de una puerta de enlace de VPN con alta disponibilidad a la interfaz 0 de la otra VPN con alta disponibilidad, y la interfaz 1 de una puerta de enlace de VPN con alta disponibilidad a la interfaz 1 de la otra VPN con alta disponibilidad.

Para obtener más información al respecto, consulte la documentación sobre las [topologías de Cloud VPN](#). Si quiere saber cómo migrar a una VPN con alta disponibilidad, consulte [este artículo](#).

Cloud Router habilita el descubrimiento dinámico de rutas entre redes conectadas



Google Cloud

Mencioné que Cloud VPN admite rutas dinámicas y estáticas. Para usar rutas dinámicas, debe configurar Cloud Router, que puede administrar rutas para un túnel de Cloud VPN mediante el protocolo de puerta de enlace fronteriza (BGP). Este método de enrutamiento permite que las rutas se actualicen y se intercambien sin modificar la configuración del túnel.

Esto permite que las nuevas subredes, como la de etapa de pruebas de la red de VPC y la del bastidor 30 de la red de intercambio de tráfico, se anuncien sin inconvenientes entre redes.

Use Cloud Interconnect cuando se necesite una conexión dedicada de alta velocidad entre las redes

- La Interconexión dedicada proporciona una conexión directa a una instalación de colocación.
 - De 10 a 200 Gbps
- La Interconexión de socio proporciona una conexión mediante un proveedor de servicios.
 - Puede comprar menos ancho de banda a partir de 50 Mbps.
- Permite acceder a los recursos de VPC con un espacio de dirección IP interna.
- El Acceso privado a Google permite que los hosts locales accedan a los servicios de Google con IP privadas.

Google Cloud

Si necesita una conexión dedicada de alta velocidad entre las redes, considere usar Cloud Interconnect. Este producto cuenta con las siguientes dos opciones para ampliar las redes locales: la Interconexión dedicada y la Interconexión de socio.

La Interconexión dedicada proporciona una conexión directa a una instalación de colocación. La instalación de colocación debe admitir circuitos de 10 o 100 Gbps. Una conexión dedicada puede incluir hasta ocho conexiones de 10 Gbps o dos de 100 Gbps para un máximo de 200 Gbps.

La Interconexión de socio proporciona una conexión mediante un proveedor de servicios. Esto puede ser útil para requisitos de ancho de banda más bajos a partir de los 50 Mbps.

En ambos casos, Cloud Interconnect permite acceder a los recursos de VPC con un espacio de dirección IP interna.

Incluso puede configurar el Acceso privado a Google para hosts locales a fin de permitirles acceder a los servicios de Google usando direcciones IP privadas.

Use Cloud Interconnect cuando se necesite una conexión dedicada de alta velocidad entre las redes

- La Interconexión dedicada proporciona una conexión directa a una instalación de colocación.
 - De 10 a 200 Gbps
- La Interconexión de socio proporciona una conexión mediante un proveedor de servicios.
 - Puede comprar menos ancho de banda a partir de 50 Mbps.
- Permite acceder a los recursos de VPC con un espacio de dirección IP interna.
- El Acceso privado a Google permite que los hosts locales accedan a los servicios de Google con IP privadas.

Si necesita una conexión dedicada de alta velocidad entre las redes, considere usar Cloud Interconnect. Este producto cuenta con las siguientes dos opciones para ampliar las redes locales: la Interconexión dedicada y la Interconexión de socio.

Use Cloud Interconnect cuando se necesite una conexión dedicada de alta velocidad entre las redes

- La Interconexión dedicada proporciona una conexión directa a una instalación de colocación.
 - De 10 a 200 Gbps
- La Interconexión de socio proporciona una conexión mediante un proveedor de servicios.
 - Puede comprar menos ancho de banda a partir de 50 Mbps.
- Permite acceder a los recursos de VPC con un espacio de dirección IP interna.
- El Acceso privado a Google permite que los hosts locales accedan a los servicios de Google con IP privadas.

La Interconexión dedicada proporciona una conexión directa a una instalación de colocación. La instalación de colocación debe admitir circuitos de 10 o 100 Gbps. Una conexión dedicada puede incluir hasta ocho conexiones de 10 Gbps o dos de 100 Gbps para un máximo de 200 Gbps.

Use Cloud Interconnect cuando se necesite una conexión dedicada de alta velocidad entre las redes

- La Interconexión dedicada proporciona una conexión directa a una instalación de colocación.
 - De 10 a 200 Gbps
- La Interconexión de socio proporciona una conexión mediante un proveedor de servicios.
 - Puede comprar menos ancho de banda a partir de 50 Mbps.
- Permite acceder a los recursos de VPC con un espacio de dirección IP interna.
- El Acceso privado a Google permite que los hosts locales accedan a los servicios de Google con IP privadas.

La Interconexión de socio proporciona una conexión mediante un proveedor de servicios. Esto puede ser útil para requisitos de ancho de banda más bajos a partir de los 50 Mbps.

Use Cloud Interconnect cuando se necesite una conexión dedicada de alta velocidad entre las redes

- La Interconexión dedicada proporciona una conexión directa a una instalación de colocación.
 - De 10 a 200 Gbps
- La Interconexión de socio proporciona una conexión mediante un proveedor de servicios.
 - Puede comprar menos ancho de banda a partir de 50 Mbps.
- [Permite acceder a los recursos de VPC con un espacio de dirección IP interna.](#)
- El Acceso privado a Google permite que los hosts locales accedan a los servicios de Google con IP privadas.

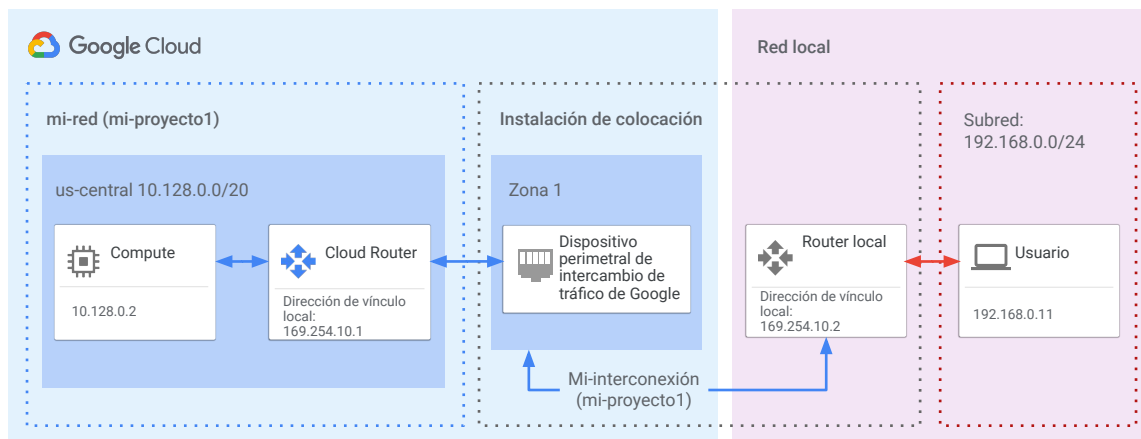
En ambos casos, Cloud Interconnect permite acceder a los recursos de VPC con un espacio de dirección IP interna.

Use Cloud Interconnect cuando se necesite una conexión dedicada de alta velocidad entre las redes

- La Interconexión dedicada proporciona una conexión directa a una instalación de colocación.
 - De 10 a 200 Gbps
- La Interconexión de socio proporciona una conexión mediante un proveedor de servicios.
 - Puede comprar menos ancho de banda a partir de 50 Mbps.
- Permite acceder a los recursos de VPC con un espacio de dirección IP interna.
- El Acceso privado a Google permite que los hosts locales accedan a los servicios de Google con IP privadas.

Incluso puede configurar el Acceso privado a Google para hosts locales a fin de permitirles acceder a los servicios de Google usando direcciones IP privadas.

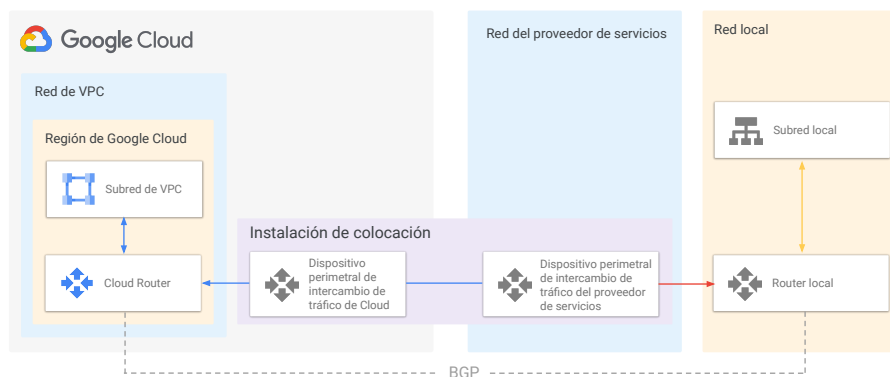
La interconexión dedicada proporciona conexiones físicas directas



Google Cloud

Para utilizar la Interconexión dedicada, debe aprovisionar una conexión cruzada entre la red de Google y su propio router en una instalación de colocación común, como se muestra en este diagrama. Para intercambiar rutas entre redes, debe configurar una sesión de BGP mediante la interconexión entre Cloud Router y el router local. Esto le permitirá al tráfico de usuarios de la red local alcanzar los recursos de Google Cloud en la red de VPC y viceversa.

La Interconexión de socio proporciona conectividad mediante un proveedor de servicios admitido



La Interconexión de socio proporciona conectividad entre su red local y la de VPC a través de un proveedor de servicios compatible. Esta es útil si su centro de datos se encuentra en una ubicación física fuera del alcance de una instalación de colocación de Interconexión dedicada o si sus necesidades de datos no justifican el uso de la Interconexión dedicada.

Actividad 9: Diseñe el diagrama de red

Consulte el cuaderno de ejercicios de Design and Process.

- Dibuje un diagrama en el que se muestren sus requisitos de red.



En esta actividad de diseño, debe dibujar un diagrama en el que se muestren los requisitos de red del caso de éxito. Veamos este ejemplo sencillo.

Actividad 9: Diseñe el diagrama de red

Consulte el cuaderno de ejercicios de Design and Process.

- Dibuje un diagrama en el que se muestren sus requisitos de red.



En esta actividad de diseño...

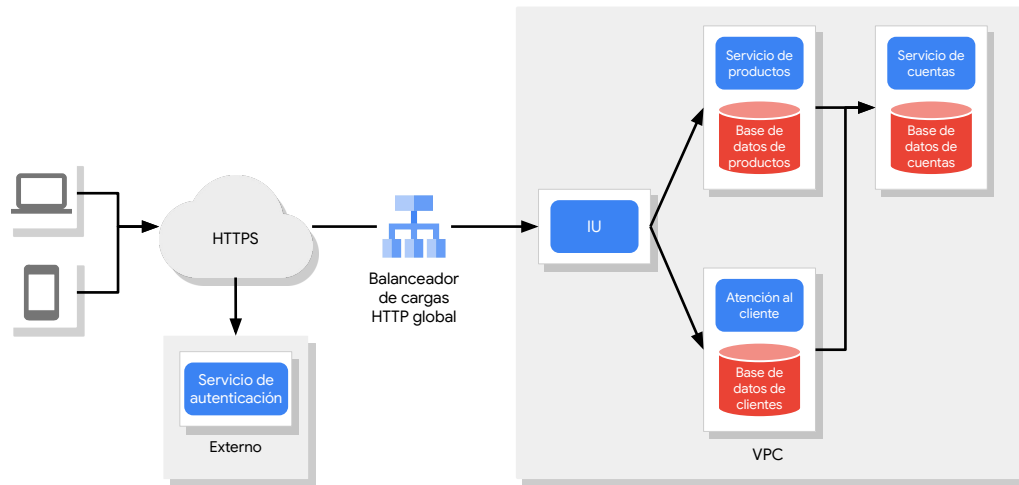
Actividad 9: Diseñe el diagrama de red

Consulte el cuaderno de ejercicios de Design and Process.

- Dibuje un diagrama en el que se muestren sus requisitos de red.



debe dibujar un diagrama en el que se muestren los requisitos de red del caso de éxito. Veamos este ejemplo sencillo.



En este diagrama, se muestran los límites de la red y cómo se entrega el tráfico de otros usuarios mediante un balanceador de cargas a nuestro backend. También podemos incluir Cloud CDN, Cloud VPN o cualquiera de los servicios de Cloud Interconnect que sean relevantes para nuestro diseño de red.

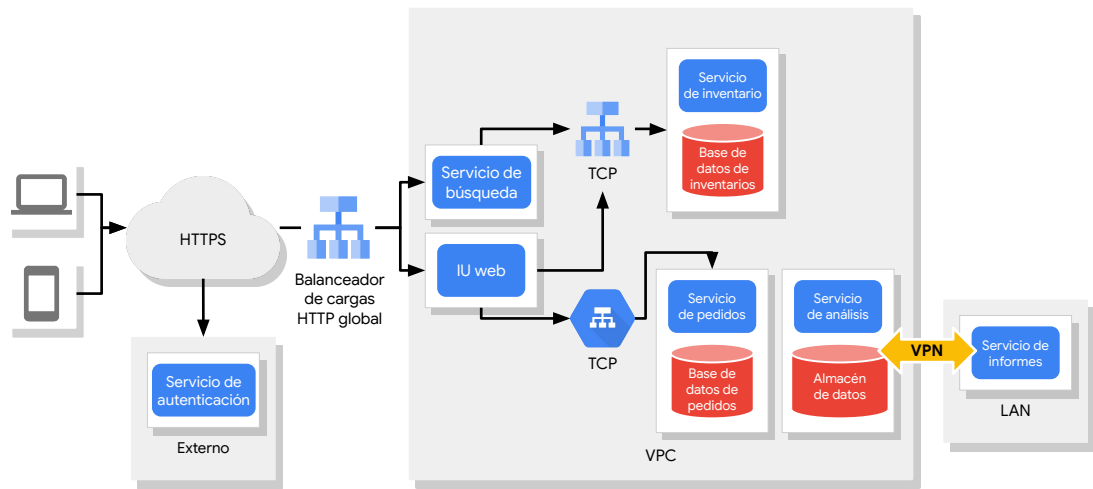
Consulte la actividad 9 del cuaderno de ejercicios a fin de crear un diagrama de red similar para sus servicios.

Revisión de la actividad 9: Diseñe el diagrama de red

- Dibuje un diagrama en el que se muestren sus requisitos de red.



En esta actividad, se le pidió crear un diagrama en el que se mostraran los requisitos de red de su aplicación.



Este es un ejemplo de TurisClic, nuestro portal de viajes en línea.

El tráfico de usuarios provenientes de dispositivos móviles y la Web se autenticará primero mediante un servicio externo. Luego, el balanceador de cargas HTTP global lo redireccionará a nuestros servicios públicos de búsqueda y de la IU web. En ese punto, los balanceadores de cargas TCP regionales dirigirán el tráfico a los servicios internos de inventario y pedidos.

El servicio de análisis puede usar BigQuery como almacén de datos con un servicio de informes local que accede a este servicio a través de una VPN. Esto puede ser suficiente para comenzar. Más adelante, podríamos definirlo mejor cuando empecemos a implementarlo.

Repaso

Google Cloud y la arquitectura de redes híbridas

En este módulo, aprendió sobre las herramientas de redes de Google Cloud y cómo diseñar redes que satisfagan los requisitos de seguridad, rendimiento, confiabilidad y escalabilidad de su aplicación.

También abordamos las diferentes opciones disponibles para conectar redes usando el intercambio de tráfico, la VPN y Cloud Interconnect.

Cuestionario

Supongamos que va a implementar una aplicación web a gran escala con usuarios de todo el mundo y mucho contenido estático. ¿Qué configuración de balanceador de cargas sería la mejor opción?

- A. Balanceador de cargas TCP con SSL configurada
- B. Balanceador de cargas HTTP con SSL configurada
- C. Balanceador de cargas HTTP con SSL configurada y CDN habilitada
- D. Balanceador de cargas UDP con SSL configurada y CDN habilitada

Supongamos que va a implementar una aplicación web a gran escala con usuarios de todo el mundo y mucho contenido estático. ¿Qué configuración de balanceador de cargas sería la mejor opción?

- A) Balanceador de cargas TCP con SSL configurada
- B) Balanceador de cargas HTTP con SSL configurada
- C) Balanceador de cargas HTTP con SSL configurada y CDN habilitada
- D) Balanceador de cargas UDP con SSL configurada y CDN habilitada

Cuestionario

Supongamos que va a implementar una aplicación web a gran escala con usuarios de todo el mundo y mucho contenido estático. ¿Qué configuración de balanceador de cargas sería la mejor opción?

- A. Balanceador de cargas TCP con SSL configurada
- B. Balanceador de cargas HTTP con SSL configurada
- C. Balanceador de cargas HTTP con SSL configurada y CDN habilitada
- D. Balanceador de cargas UDP con SSL configurada y CDN habilitada

- A. Incorrecto. Los balanceadores de cargas TCP no están diseñados para el tráfico HTTP(S). Además, el contenido estático sugiere el uso de una CDN, que no es compatible con los balanceador de cargas TCP.
- B. Incorrecto. Si bien un balanceador de cargas HTTP con SSL configurada es una buena opción, no es la mejor, ya que la CDN no está habilitada, lo que podría ayudar con la gran cantidad de contenido estático.
- C. Correcto. El tráfico es HTTP(S), el balanceador de cargas debe ser externo y global, y la CDN habilitada ayudaría con el rendimiento y los costos.
- D. Incorrecto. El tipo de tráfico no es UDP. Además, los balanceadores de cargas UDP no son globales.

C es la respuesta correcta. El tráfico es HTTP(S), el balanceador de cargas debe ser externo y global, y la CDN habilitada ayudaría con el rendimiento y los costos.

La respuesta A es incorrecta. Los balanceadores de cargas TCP no están diseñados para el tráfico HTTP(S). Además, el contenido estático sugiere el uso de una CDN, que no es compatible con los balanceador de cargas TCP.

La respuesta B es incorrecta. Si bien un balanceador de cargas HTTP con SSL configurada es una buena opción, no es la mejor, ya que la CDN no está habilitada, lo que podría ayudar con la gran cantidad de contenido estático.

La respuesta D es incorrecta. El tipo de tráfico no es UDP. Además, los balanceadores de cargas UDP no son globales.

Cuestionario

Supongamos que trabaja para un banco importante que implementará un servicio de banca en línea en Google Cloud. El servicio necesita un acceso de gran volumen a datos de unidades centrales de forma local. ¿Qué opción de conectividad sería la mejor?

- A. VPN
- B. HTTPS
- C. Cloud Interconnect
- D. Intercambio de tráfico

Supongamos que trabaja para un banco importante que implementará un servicio de banca en línea en Google Cloud. El servicio necesita un acceso de gran volumen a datos de unidades centrales de forma local. ¿Qué opción de conectividad sería la mejor?

- A. VPN
- B. HTTPS
- C. Cloud Interconnect
- D. Intercambio de tráfico

Cuestionario

Supongamos que trabaja para un banco importante que implementará un servicio de banca en línea en Google Cloud. El servicio necesita un acceso de gran volumen a datos de unidades centrales de forma local. ¿Qué opción de conectividad sería la mejor?

A. VPN

B. HTTPS

C. Cloud Interconnect

D. Intercambio de tráfico

A) Incorrecto. Una VPN es una opción para volúmenes de datos reducidos.

B) Incorrecto. HTTPS no podría brindar el ancho de banda necesario, se podrían generar costos de Internet y el tráfico migraría a la Internet pública.

C) Correcto. Cloud Interconnect proporciona un ancho de banda alto con baja latencia. Sin embargo, se necesita encriptación a nivel de la aplicación.

D) Incorrecto. El intercambio de tráfico es para la conectividad de servicios como G Suite.

C es la respuesta correcta. Cloud Interconnect proporciona un ancho de banda alto con baja latencia. Sin embargo, se necesita encriptación a nivel de la aplicación.

La respuesta A es incorrecta. Una VPN es una opción para volúmenes de datos reducidos.

La respuesta B es incorrecta. HTTPS no podría brindar el ancho de banda necesario, se podrían generar costos de Internet y el tráfico migraría a la Internet pública.

La respuesta D es incorrecta. El intercambio de tráfico es para la conectividad de servicios como G Suite.

Cuestionario

Supongamos que tiene un contrato con un proveedor de servicios para administrar sus redes de VPC de Google y quiere conectar una de las redes de este proveedor a su VPC. Ambas redes están en Google Cloud. ¿Qué opción de conexión elegiría?

- A. VPN
- B. VPN con alta disponibilidad y Cloud Router
- C. Cloud Interconnect
- D. Intercambio de tráfico entre VPC

Supongamos que tiene un contrato con un proveedor de servicios para administrar sus redes de VPC de Google y quiere conectar una de las redes de este proveedor a su VPC. Ambas redes están en Google Cloud. ¿Qué opción de conexión elegiría?

- A. VPN
- B. VPN con alta disponibilidad y Cloud Router
- C. Cloud Interconnect
- D. Intercambio de tráfico entre VPC

Cuestionario

Supongamos que tiene un contrato con un proveedor de servicios para administrar sus redes de VPC de Google y quiere conectar una de las redes de este proveedor a su VPC. Ambas redes están en Google Cloud. ¿Qué opción de conexión elegiría?

- A. VPN
- B. VPN con alta disponibilidad y Cloud Router
- C. Cloud Interconnect
- D. Intercambio de tráfico entre VPC

Las respuestas A, B y C son incorrectas. Todas se diseñaron para conectar redes externas a una VPC.

D) Correcto. El intercambio de tráfico de VPC permite la conectividad en dos redes de VPC, independientemente de si pertenecen al mismo proyecto o a la misma organización.

D es la respuesta correcta. El intercambio de tráfico de VPC permite la conectividad en dos redes de VPC, independientemente de si pertenecen al mismo proyecto o a la misma organización.

Las respuestas A, B y C son incorrectas. Todas se diseñaron para conectar redes externas a una VPC.

Cuestionario

Supongamos que necesita una conexión privada y segura entre su red y una red de Google Cloud. Si bien no tiene mucho volumen de datos, la conexión debe ser extremadamente confiable. ¿Cuál de los siguientes parámetros de configuración elegiría?

- A. VPN
- B. VPN con alta disponibilidad y Cloud Router
- C. Cloud Interconnect
- D. Intercambio de tráfico entre VPC

Supongamos que necesita una conexión privada y segura entre su red y una red de Google Cloud. Si bien no tiene mucho volumen de datos, la conexión debe ser extremadamente confiable. ¿Cuál de los siguientes parámetros de configuración elegiría?

- A. VPN
- B. VPN con alta disponibilidad y Cloud Router
- C. Cloud Interconnect
- D. Intercambio de tráfico entre VPC

Cuestionario

Supongamos que necesita una conexión privada y segura entre su red y una red de Google Cloud. Si bien no tiene mucho volumen de datos, la conexión debe ser extremadamente confiable. ¿Cuál de los siguientes parámetros de configuración elegiría?

- A. VPN
- B. VPN con alta disponibilidad y Cloud Router
- C. Cloud Interconnect
- D. Intercambio de tráfico entre VPC

A) Incorrecto. Si bien la VPN es una opción de conectividad adecuada, no ofrece una alta disponibilidad.

B) Esta es la opción correcta, ya que ofrece una conexión segura y extremadamente confiable, y es más rentable que Cloud Interconnect.

C) Incorrecto. Cloud Interconnect es para cantidades grandes de datos.

D) Incorrecto. El intercambio de tráfico de VPC se utiliza para la interconexión de dos redes de VPC.

B es la respuesta correcta. ya que ofrece una conexión segura y extremadamente confiable, y es más rentable que Cloud Interconnect.

La respuesta A es incorrecta. Si bien la VPN es una opción de conectividad adecuada, no ofrece una alta disponibilidad.

La respuesta C es incorrecta. Cloud Interconnect es para cantidades grandes de datos.

La respuesta D es incorrecta. El intercambio de tráfico de VPC se utiliza para la

interconexión de dos redes de VPC.

Más recursos

Productos de Herramientas de redes de Cloud

<https://cloud.google.com/products/networking/>

Conectividad híbrida de Google Cloud

<https://cloud.google.com/hybrid-connectivity/>

Los vínculos otorgan acceso a algunos recursos útiles sobre las herramientas de redes de Google Cloud.