Renuncia de responsabilidad

Gracias por su interés en usar el material de capacitación de Google Cloud. Nos complace poder brindarle el siguiente contenido (en adelante, los "Recursos Didácticos") y esperamos que le resulte útil.

Al usar los Recursos didácticos, acepta regirse por los siguientes términos y condiciones, así como las Condiciones del Servicio de Google y la Política de Privacidad de Google. A menos que se indique lo contrario, los términos que se usan a continuación tendrán los significados que se describen en las Condiciones del Servicio de Google.

1. **Solo para usos educativos.** Los Recursos Didácticos están diseñados para utilizarse solo en los cursos de capacitación que se dictan en instituciones de educación superior o con acreditación regional. El contenido puede adaptarse, personalizarse, modificarse y compartirse para fines educativos. Sin embargo, no puede distribuirse ni usarse de otro modo para fines comerciales ni para obtener un beneficio comercial o una compensación económica de carácter privado.

1. **Requisitos de atribución.** Si distribuye, reproduce públicamente, exhibe, transmite o publica los Recursos Didácticos o sus obras derivadas, o hace que estén disponibles de otro modo, deberá atribuir el material que utilice a los Recursos Didácticos, pero no deberá hacerlo de forma que sugiera que Google, sus afiliados o sus proveedores de contenido de terceros lo respaldan o aprueban que use dichos materiales. Si adapta, modifica o personaliza los Recursos Didácticos, deberá incluir el siguiente texto en cada una de las diapositivas modificadas: *"El contenido original que suministra Google LLC se modificó para los fines de este curso sin participación ni recomendación de Google LLC"*.

1. Las descripciones de los productos, la infraestructura y los servicios de Google disponibles en los Recursos Didácticos se incluyen solo para fines de aprendizaje y no constituyen una garantía, una promesa ni una declaración de exactitud por parte de Google. Los precios, la disponibilidad o las funciones de los productos y servicios de Google Cloud que se describen en los Recursos Didácticos pueden cambiar.

Diagrama del curso

Google Cloud

La nube no es segura, ¿verdad?

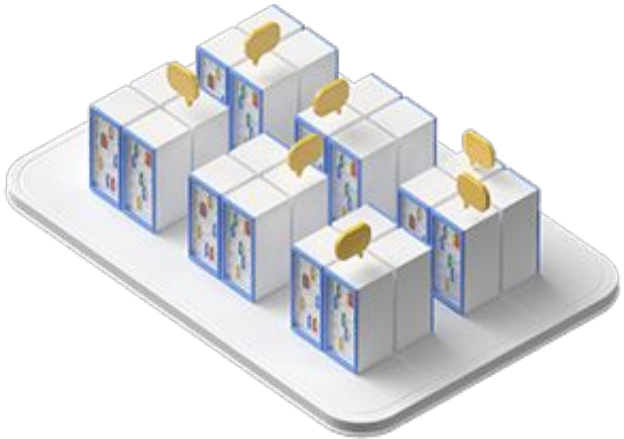
Capas de seguridad de la infraestructura de Google

Cómo proteger la infraestructura de bajo nivel

- Centros de datos de última generación
- Seguridad de las instalaciones físicas
- Diseño y origen del hardware
- Identidad de las máquinas y pila de inicio seguras

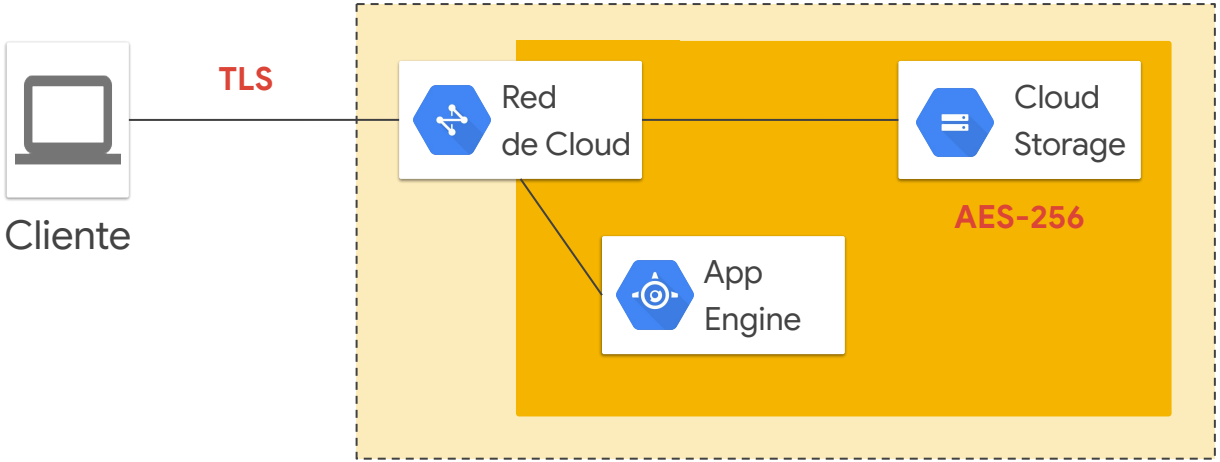
Cómo proteger la implementación del servicio

- Identidad, integridad y aislamiento de los servicios y administración del acceso entre servicios
- Encriptación de la comunicación entre servicios
- Programas externos de recompensas por detección de errores



Opciones de Encriptación

Google Cloud proporciona encriptación en el lado del servidor



Hay varias opciones de encriptación

Más simples

Con mayor control

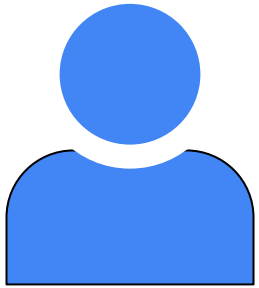
Encriptación predeterminada (solo en Google Cloud)

Claves de encriptación administradas por el cliente

Claves de encriptación proporcionadas por el cliente

Autenticación y autorización AIM

Cloud Identity and Access Management permite a los administradores autorizar quién puede actuar sobre recursos específicos

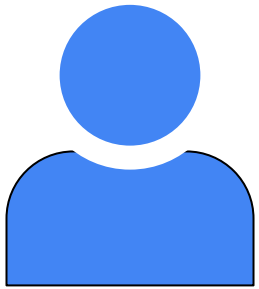


Quién

puede hacer qué

con qué recurso

Quién: Las políticas de IAM pueden aplicarse a cualquiera de los cuatro tipos de fuentes de usuario



Quién

Cuenta de Google o usuario de Cloud Identity
test@gmail.com test@example.com

Cuenta de servicio
test@project_id.iam.gserviceaccount.com

Grupos de Google
test@googlegroups.com

G Suite

Dominio de Cloud Identity o G Suite
example.com

Qué puede hacer: Las funciones de IAM son colecciones de permisos relacionados

Qué puede hacer

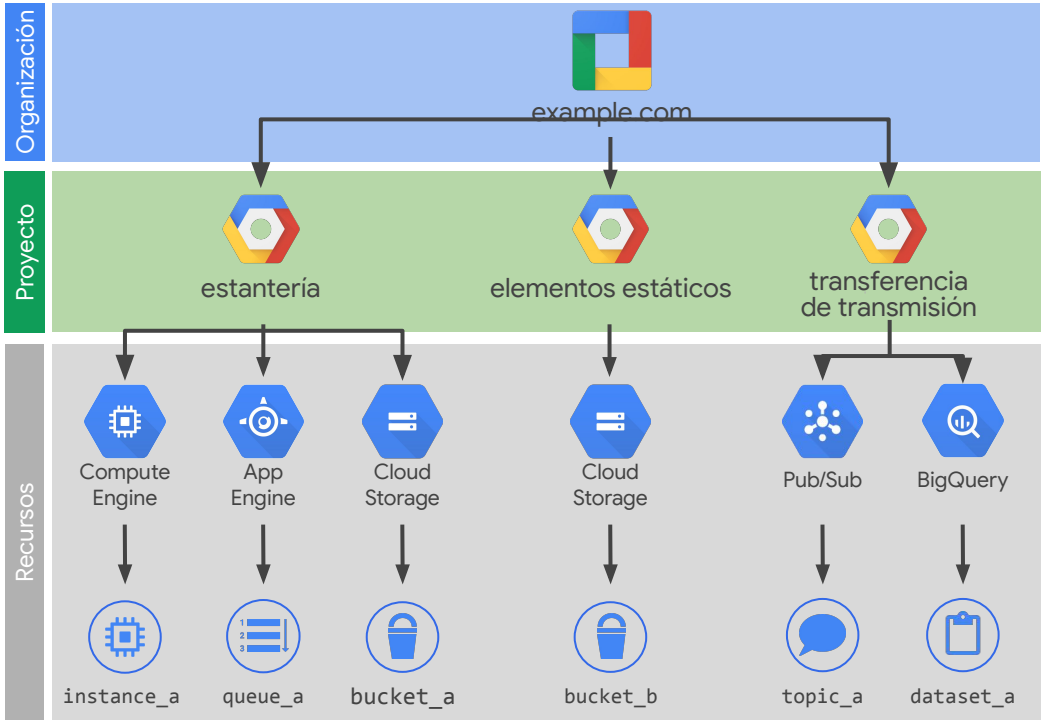
InstanceAdmin

Función

Servicio	Recurso	Verbo
procesamiento	*instancias*	*hacer una lista*
procesamiento	*instancias*	*borrar*
procesamiento	*instancias*	*iniciar*
...		

Sobre qué recurso: Los usuarios obtienen funciones sobre elementos específicos en la jerarquía

con qué recurso



¿Qué tal si ya existe un directorio corporativo diferente?

Microsoft Active Directory o LDAP

Usuarios y grupos en el servicio de directorio existente

Cloud Directory Sync de Google

Sincronización programada en una sola dirección

Usuarios y grupos en su dominio de Cloud Identity

Existen tres tipos de funciones de IAM

Básicas

Predefinidas

Personalizadas

Las funciones básicas de IAM ofrecen niveles de acceso fijos poco específicos

Propietario

- Invita miembros.
- Quita miembros.
- Borra proyectos.
- Además de lo que pueden hacer el Editor y el Lector.

Editor

- Implementa aplicaciones.
- Modifica el código.
- Configura servicios.
- Además de lo que puede hacer el lector.

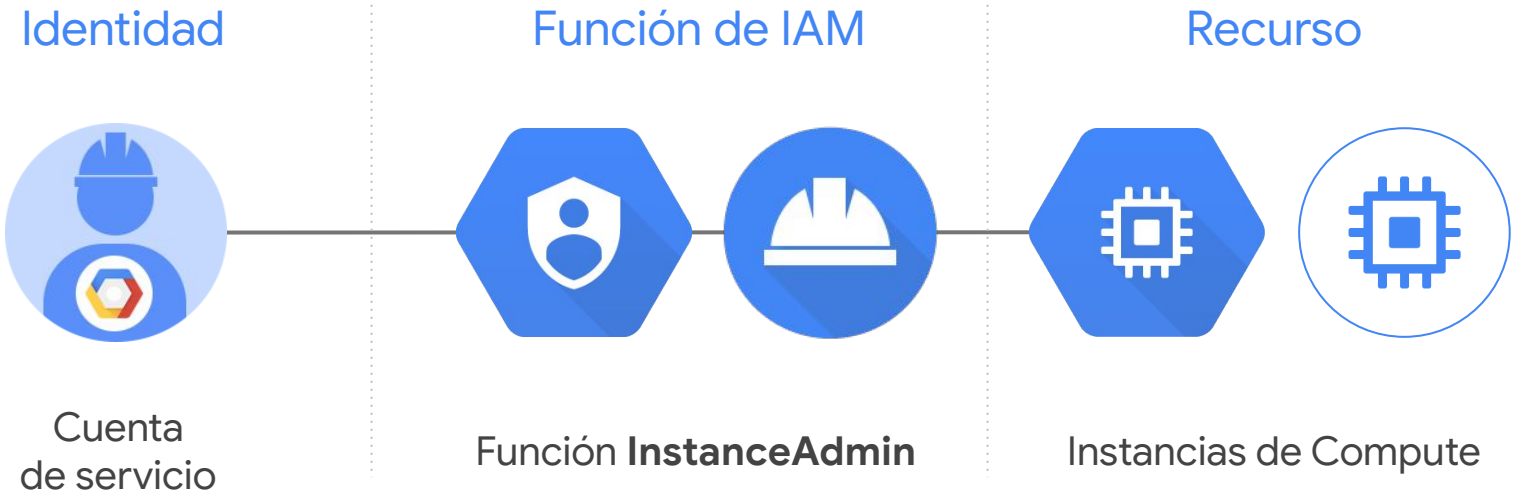
Lector

- Tiene acceso de solo lectura.

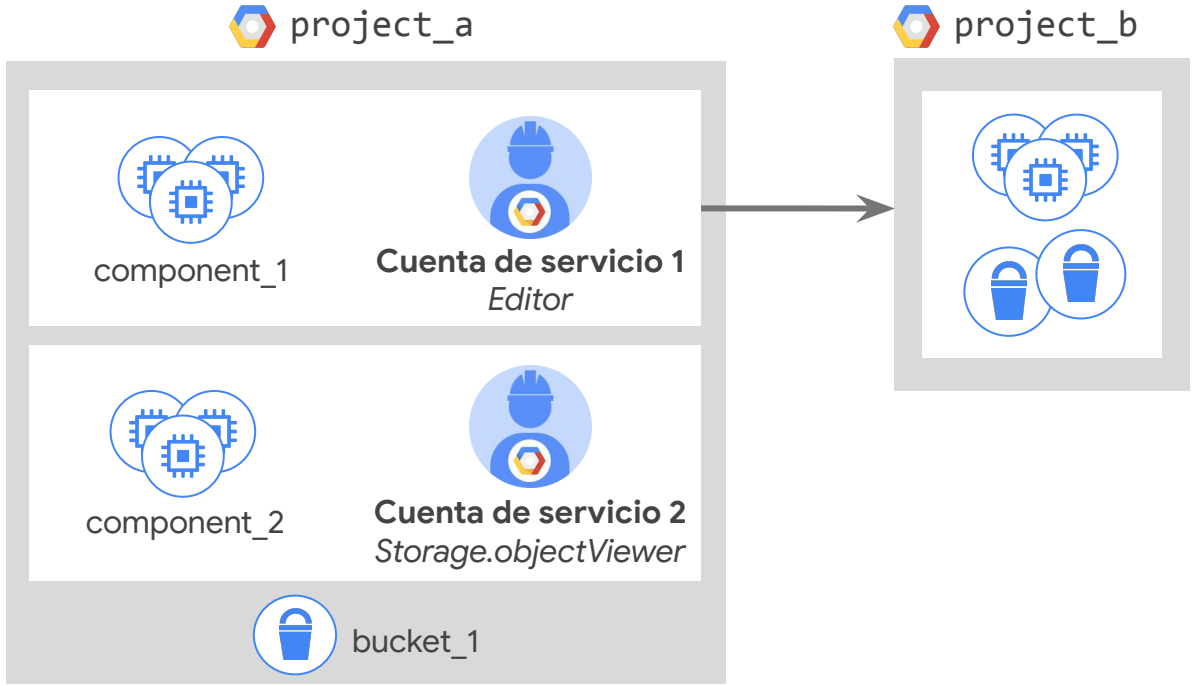
Administrador de facturación

- Administra la facturación.
- Agrega y quita administradores.

Cuentas de servicio y IAM



Puede otorgarles diferentes identidades a distintos grupos de VM en un proyecto



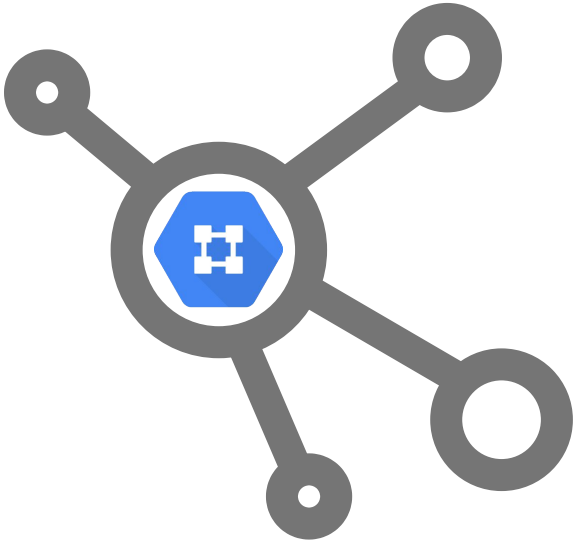
Redes

Las herramientas de redes en contexto

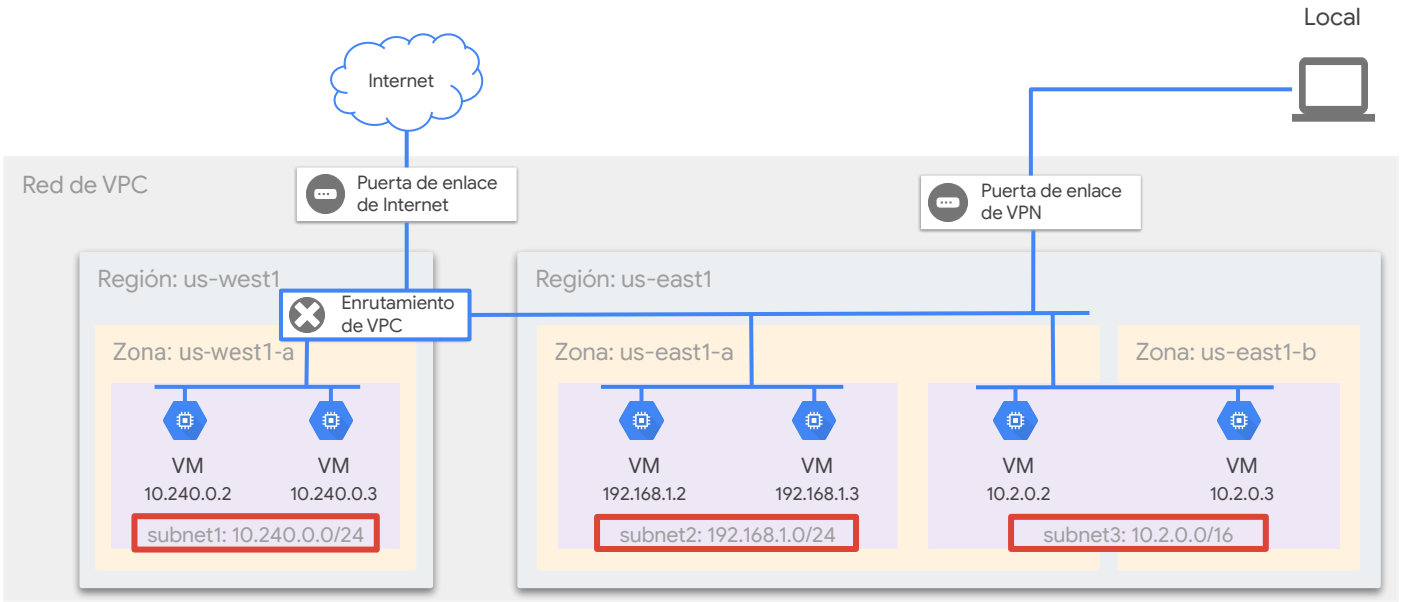
Redes privadas

Las VPC son construcciones de red definidas por software (SDN)

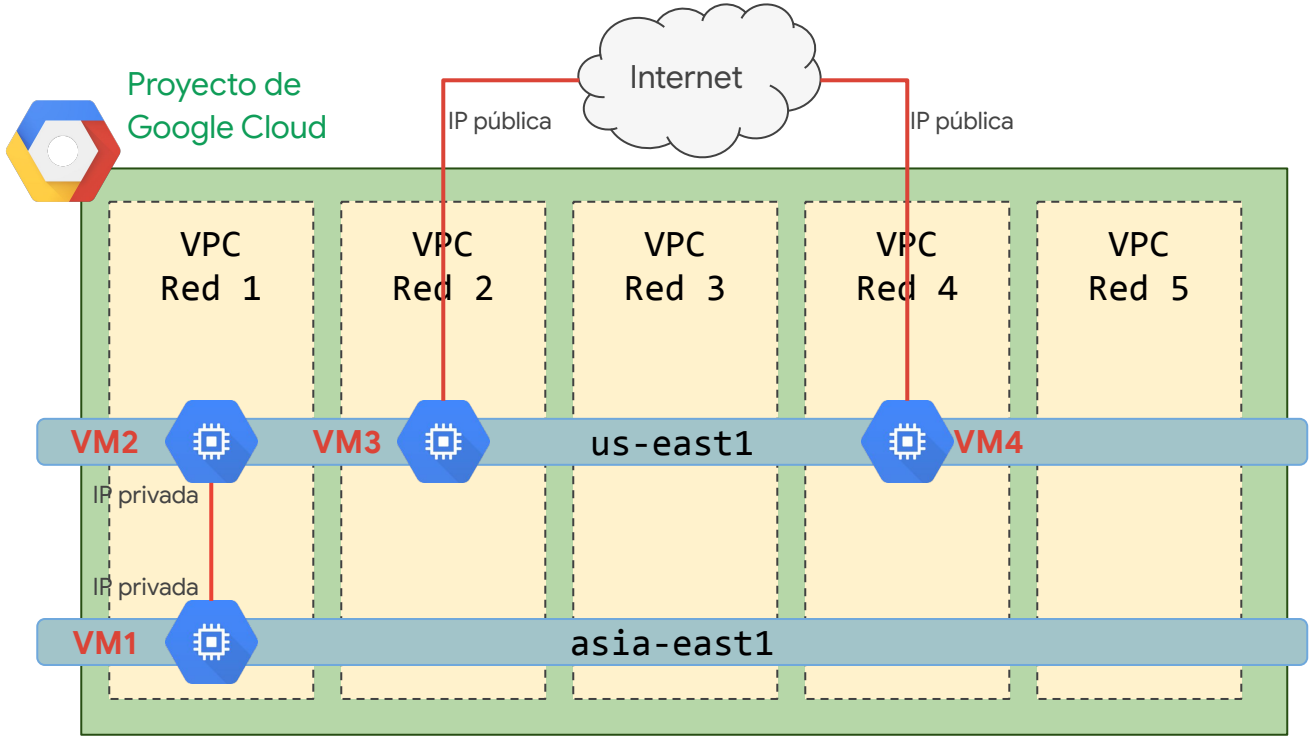
- Permiten la implementación de recursos de IaaS.
- No tienen rangos de direcciones IP.
- Son globales.
- Contienen subredes.



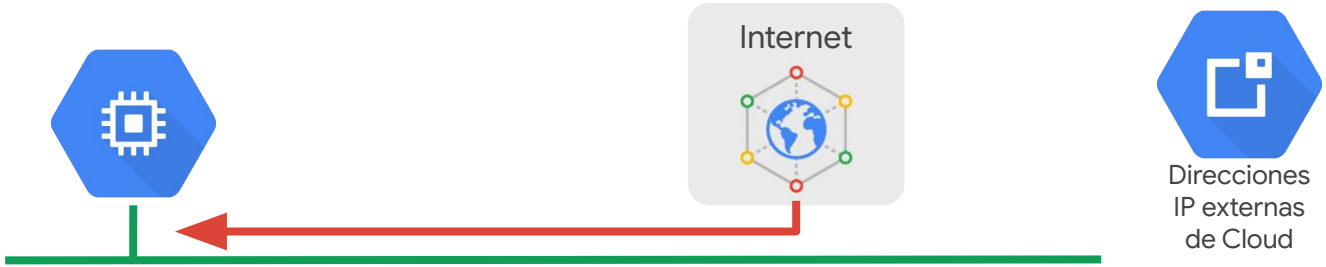
Una red de VPC es una versión virtual de una red física y es un recurso global



Comportamiento de la red dentro de un proyecto



Aspectos básicos de las direcciones IP públicas y privadas



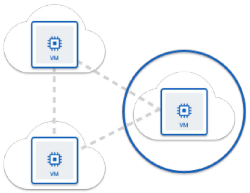
IP interna

- Se asigna del rango de subred a las VM mediante DHCP.
- La asignación de tiempo de DHCP se renueva cada 24 horas.
- El nombre de la VM y la IP se registran con un DNS acotado a la red.

IP externa

- Se puede asignar desde un grupo (efímera) o se puede reservar (estática).
- Se factura cuando no está vinculada a una VM en ejecución.
- La VM no conoce la IP externa; está asignada a la IP interna.

Los principales productos que incluyen las herramientas de red de Google

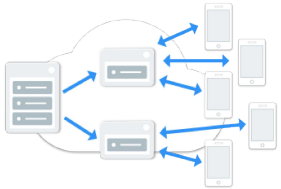


Nube privada virtual

Administración de herramientas de redes para recursos

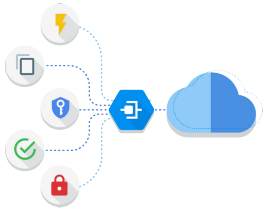
Balanceador de cargas de Cloud

Ajuste de escala automático y balanceo de cargas en todo el mundo



Cloud CDN

Red de distribución de contenidos



Cloud Interconnect

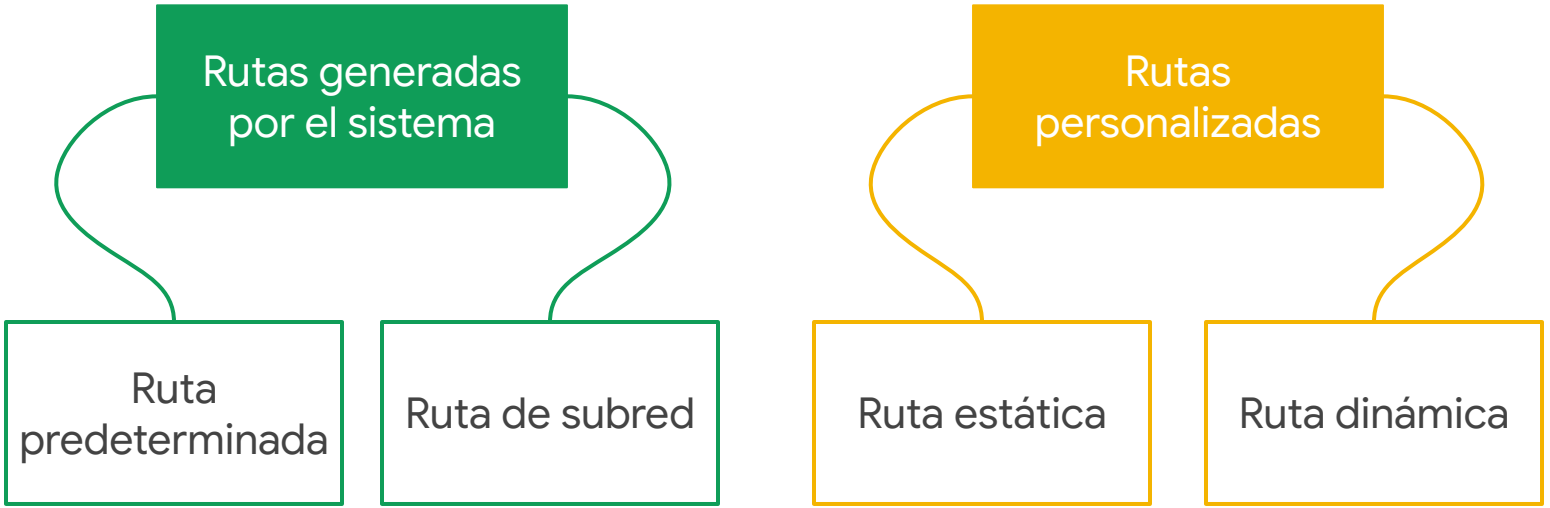
Interconexión rápida y de alta disponibilidad

Cloud DNS

Red de DNS global con alta disponibilidad

Rutas y reglas de firewall

Existen cuatro tipos de rutas diferentes



El firewall protege las instancias de máquinas virtuales contra conexiones no aprobadas

- La red de VPC funciona como un firewall distribuido.
- Las reglas de firewall se aplican a toda la red.
- Las conexiones se permiten o se rechazan a nivel de la instancia.
- Las reglas de firewall tienen estado.
- Las reglas implícitas rechazan todas las entradas y permiten todas las salidas.

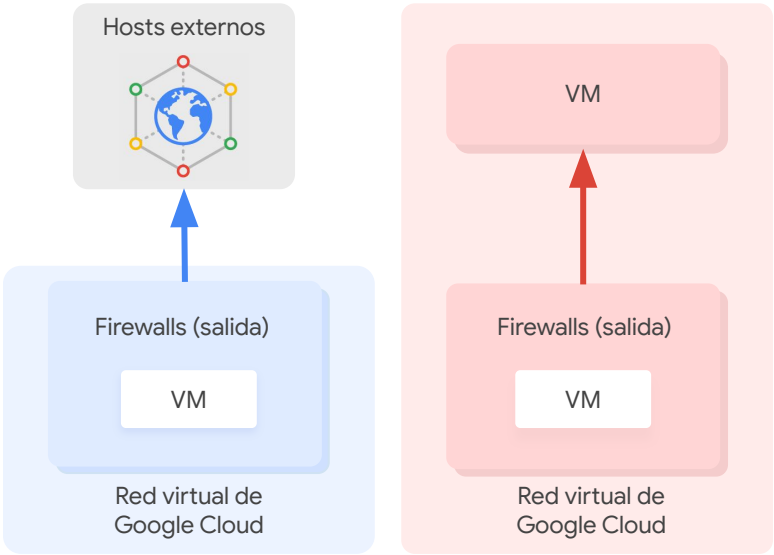
Caso de uso del firewall de Google Cloud: salida

Condiciones:

- Rangos de CIDR de destino
- Protocolos
- Puertos

Acción:

- Permitir: admite la conexión de salida coincidente
- Rechazar: bloquea la conexión de salida coincidente



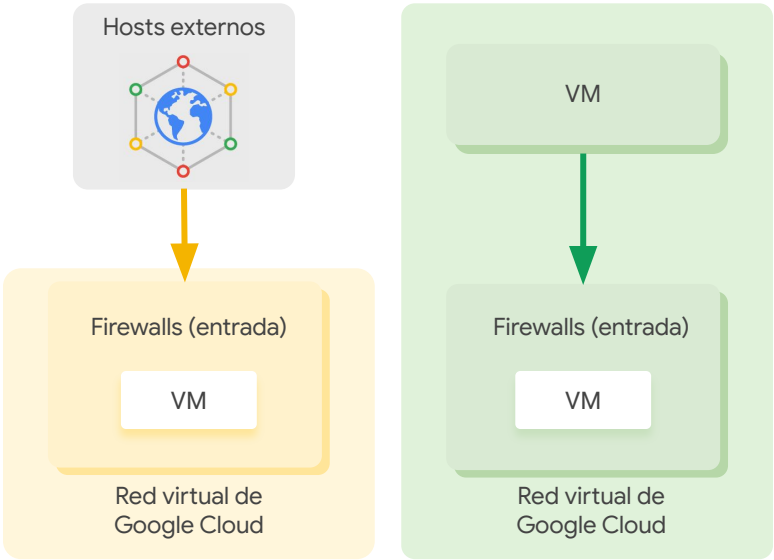
Caso de uso del firewall de Google Cloud: entrada

Condiciones:

- Rangos de CIDR de origen
- Protocolos
- Puertos

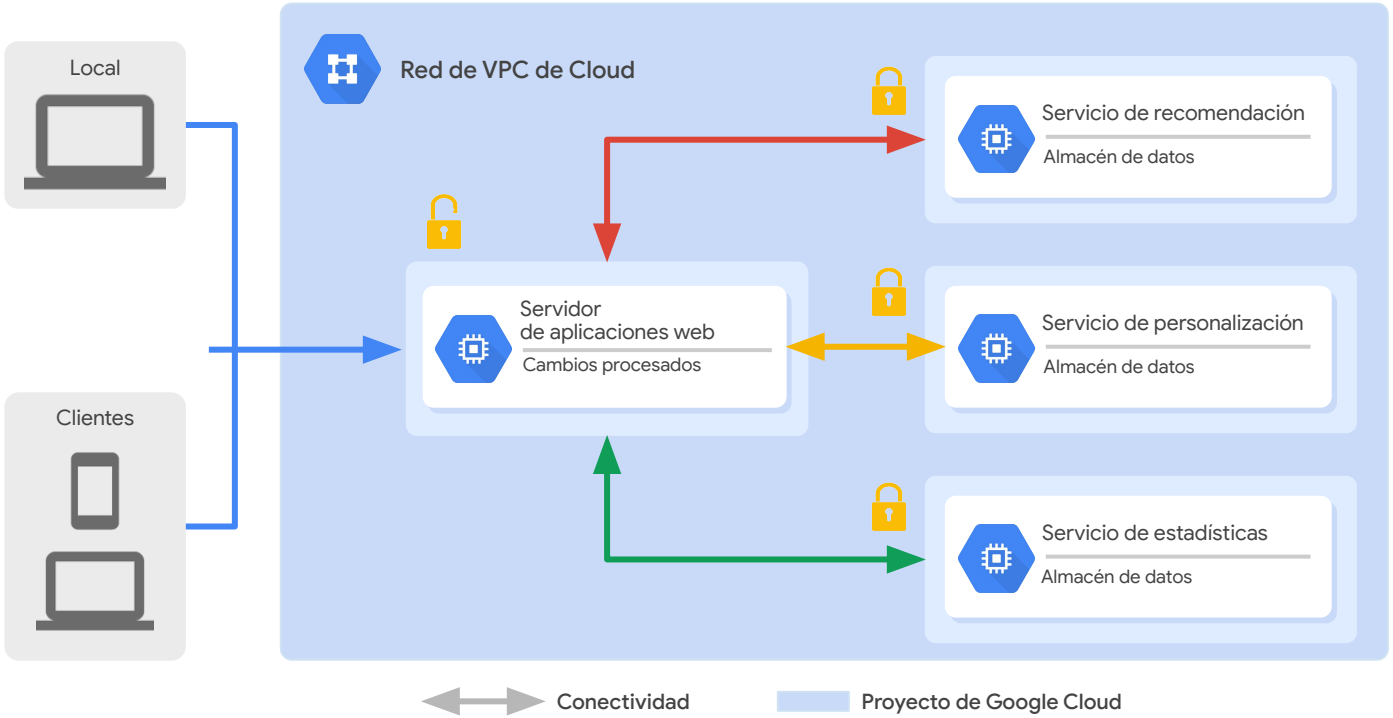
Acción:

- Permitir: admite la conexión de entrada coincidente
- Rechazar: bloquea la conexión de entrada coincidente



Redes de VPC múltiples

Conecte recursos de varios proyectos a una red de VPC común



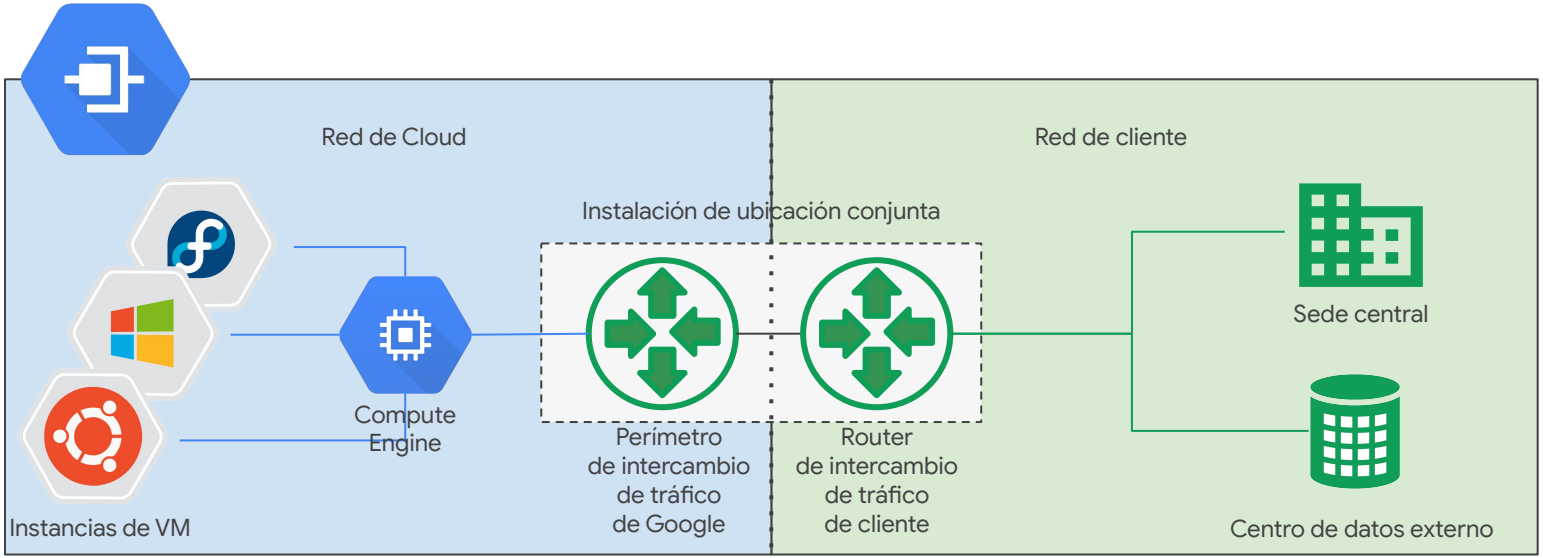
Google Cloud

Cómo conectar nubes híbridas

Comparación entre las opciones de interconexión

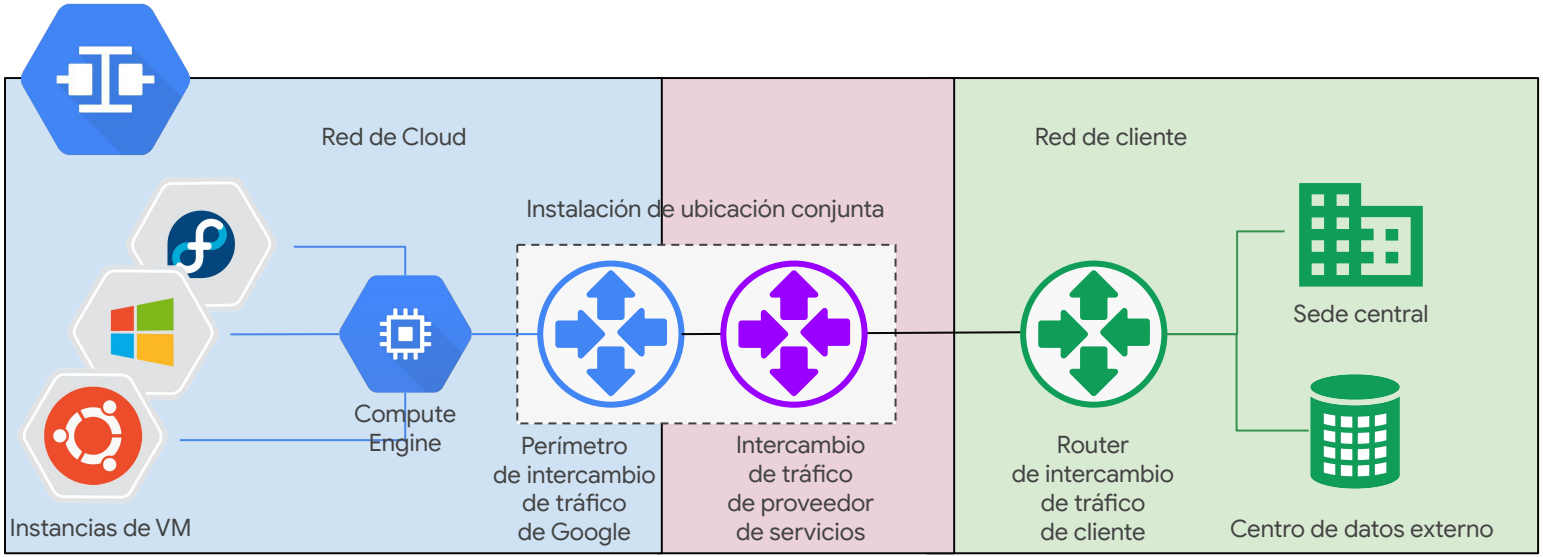
Conexión	Proporciona	Capacidad	Requisitos	Tipo de acceso
Túneles VPN IPsec	Túnel encriptado para redes de VPC a través de la Internet pública	Entre 1.5 Gbps y 3.0 Gbps por túnel	Puerta de enlace de VPN local	Direcciones IP internas
Interconexión dedicada	Conexión dedicada y directa a redes de VPC	8 circuitos de 10 Gbps 2 circuitos de 100 Gbps por conexión	Conexión en una instalación de colocación	Direcciones IP internas
Interconexión de socio	Ancho de banda dedicado, conexión a la red de VPC a través de un proveedor de servicios	Entre 50 Mbps y 10 Gbps por conexión	Proveedor de servicios	Direcciones IP internas

Interconexión dedicada



Una red

Interconexión de socio



IAC

Puede definir su infraestructura requerida como código

- Los requisitos de la infraestructura se definen como código en una plantilla que tiene un formato legible para las personas y que las máquinas pueden procesar.
- Utilice las plantillas para automatizar la compilación, modificación y eliminación de la infraestructura.
- Las plantillas se pueden almacenar, versionar y compartir.
- Las plantillas se pueden utilizar para volver a compilar una infraestructura tras una falla.

La asistencia de Google Cloud también está disponible para herramientas de IaC de código abierto de terceros

Deployment Manager

HashiCorp Terraform

puppet

ANSIBLE

HashiCorp Packer

CHEF™

Google Cloud's Operations Suite

Google Cloud's operations suite