



En este módulo, analizaremos las redes virtuales.

Google Cloud usa una red definida por software y desarrollada en una infraestructura global de fibra óptica. Esta infraestructura hace que Google Cloud tenga una de las redes más grandes y rápidas del mundo. Si considera los recursos como servicios (en lugar de hardware), podrá comprender las opciones disponibles y cómo funcionan.

# Temario

---

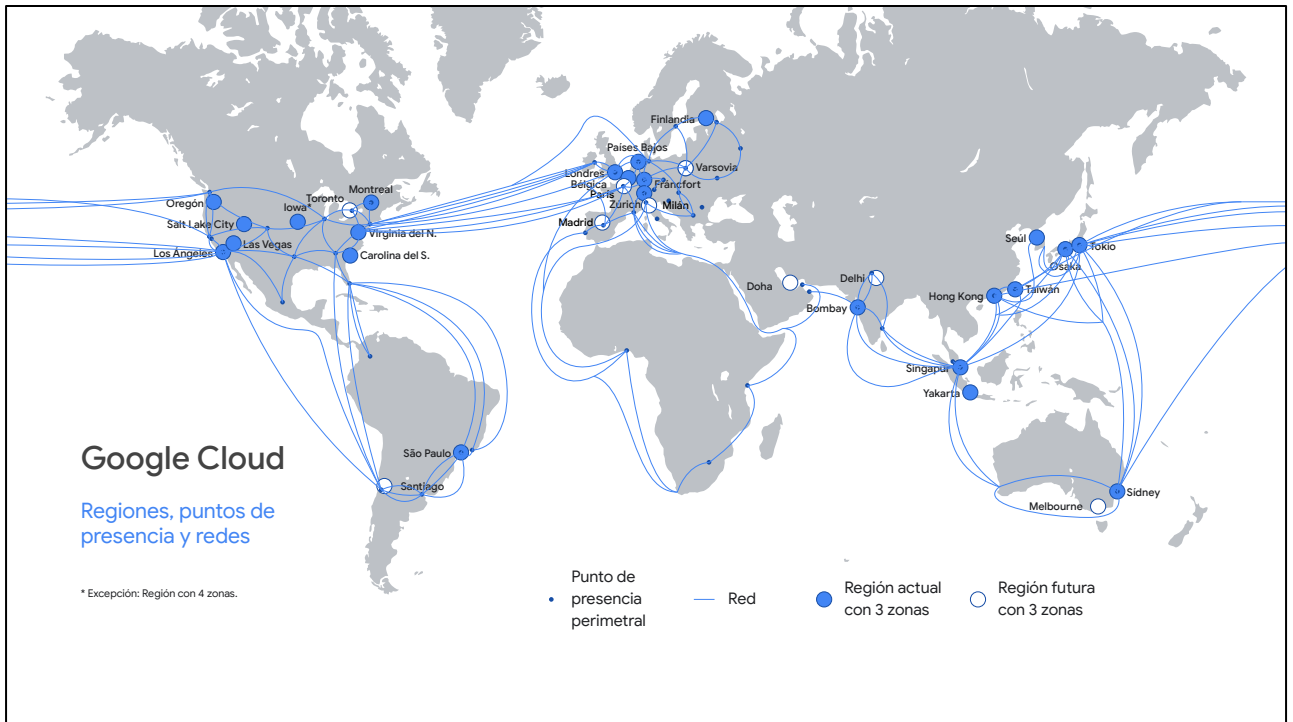
- Nube privada virtual (VPC)
- Proyectos, redes y subredes
- Direcciones IP
- Rutas y reglas de firewall
- Precios
- Lab
- Diseños comunes de redes
- Lab



Comenzaremos el módulo con una presentación de la nube privada virtual (VPC), que es la funcionalidad de redes administradas de Google para sus recursos de Cloud Platform. Luego, desglosaremos las redes en sus componentes fundamentales: proyectos, redes, subredes, direcciones IP, rutas y reglas de firewall, y analizaremos los precios de red.

A continuación, exploraremos la estructura de red de Google Cloud a través de un lab en el que crearemos redes de muchas variedades diferentes y analizaremos las relaciones entre ellas.

Después de eso, observaremos diseños de redes comunes.



Este mapa representa a Google Cloud. En el nivel general, Google Cloud está compuesto por regiones (íconos azules), puntos de presencia o PoP (puntos azules), 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. Las regiones marcadas con íconos azules tienen tres zonas. La única excepción es Iowa, cuya región us-central1 tiene cuatro zonas: us-central1-a, us-central1-b, us-central1-c y us-central1-f. Para obtener información actualizada sobre las regiones y zonas, consulte la página de documentación que se indica en las diapositivas. [<https://cloud.google.com/compute/docs/regions-zones/>]

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. Para obtener más información sobre la infraestructura de red de Google, consulte las diapositivas. [<https://peering.google.com/#/infrastructure>]

# Temario

---

## Nube privada virtual (VPC)

Proyectos, redes y subredes

Direcciones IP

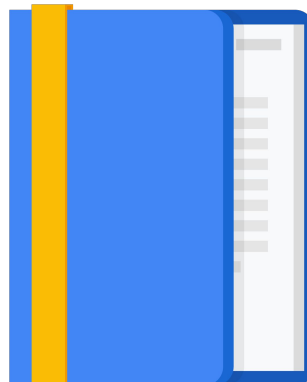
Rutas y reglas de firewall

Precios

Lab

Diseños comunes de redes

Lab



Para comenzar, hablemos sobre la red de Google Cloud y, específicamente, sobre la nube privada virtual (VPC).

## Objetos de VPC



- Proyectos
- Redes
  - Predeterminada, modo automático, modo personalizado
- Subredes
- Regiones
- Zonas
- Direcciones IP
  - Interna, externa, rango
- Máquinas virtuales (VMs)
- Rutas
- Reglas de firewall

Con Google Cloud, puede aprovisionar sus recursos del servicio, conectarlos a otros y aislarlos en una nube privada virtual. También puede definir políticas detalladas de red en Google Cloud, y entre Google Cloud y otros entornos locales o nubes públicas. En términos simples, VPC es un conjunto integral de objetos de red administrados por Google que analizaremos en detalle en este módulo.

Primero, veamos una descripción general de los objetos:

- Los proyectos abarcarán todos los servicios que use, incluidas las redes.
  - Existen tres tipos de redes: predeterminadas, de modo automático y de modo personalizado.
  - Las subredes le permiten dividir o segregar su entorno.
  - Las regiones y las zonas representan los centros de datos de Google y proporcionan alta disponibilidad y protección continua de los datos.
  - VPC ofrece direcciones IP para uso interno y externo, además de selecciones detalladas de rangos de direcciones IP.
- En cuanto a las máquinas virtuales, en este módulo nos enfocaremos en configurar instancias de VM desde la perspectiva de las redes.
- También analizaremos las rutas y las reglas de firewall.

# Temario

---

Nube privada virtual (VPC)

Proyectos, redes y subredes

Direcciones IP

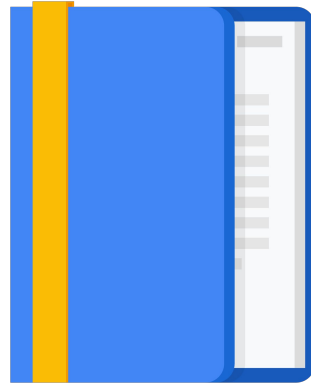
Rutas y reglas de firewall

Precios

Lab

Diseños comunes de redes

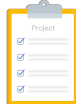
Lab



En primer lugar, hablemos sobre los proyectos, las redes y las subredes para analizar los objetos de VPC.

# Proyectos y redes

## Características de los proyectos:



- Asocian objetos y servicios con facturación.
- Contienen redes (hasta 5) que se pueden compartir o intercambiar.

## Características de las redes:



- No tienen rangos de direcciones IP.
- Son globales y abarcan todas las regiones disponibles.
- Contienen subredes.
- Están disponibles como predeterminadas, automáticas o personalizadas.

Google Cloud

Los proyectos son el elemento organizador clave de los recursos de infraestructura en Google Cloud. Los proyectos asocian los objetos y servicios con la facturación. Lo que los hace únicos es que, en realidad, pueden contener redes completas. La cuota predeterminada para cada proyecto es de 5 redes, pero puede solicitar fácilmente un aumento con Cloud Console. Estas redes se pueden compartir con otros proyectos o pueden intercambiar tráfico con redes de otros proyectos. Analizaremos ambas opciones en la serie de cursos Architecting with Google Compute Engine.

Las redes no tienen rangos de IP, ya que son solo una construcción de todos los servicios y las direcciones IP individuales en ella. Las redes de Google Cloud son globales, es decir, abarcan todas las regiones disponibles en el mundo que se mostraron anteriormente. Por lo tanto, puede tener una red que literalmente exista en todo el mundo a la vez: Asia, Europa, América, etcétera.

En una red, puede segregar sus recursos con subredes regionales.

Hace un momento, mencionamos que existen distintos tipos de redes: predeterminadas, automáticas y personalizadas. Analicémoslas en profundidad.

## 3 tipos de redes de VPC



Google Cloud

Todos los proyectos cuentan con una red de VPC predeterminada, que tiene subredes y reglas de firewall predefinidas. Específicamente, se asigna una subred a cada región con bloques CIDR no superpuestos y reglas de firewall que permiten tráfico de entrada de ICMP, RDP y SSH desde cualquier lugar, además de tráfico de entrada desde la red predeterminada para todos los protocolos y puertos.

En las redes de modo automático, se crea automáticamente una subred de cada región dentro de ella. En realidad, las redes predeterminadas son redes de modo automático. Estas subredes que se crearon automáticamente usan un conjunto de rangos de IP predefinidos con una máscara /20 que se puede expandir a /16. Todas estas subredes se ajustan al bloque CIDR 10.128.0.0/9. Por lo tanto, a medida que están disponibles las nuevas regiones de Google Cloud, se agregan automáticamente las subredes nuevas en esas regiones a las redes de modo automático con un rango de IP de ese bloque.

Las redes en modo personalizado no crean subredes automáticamente. Este tipo de red le proporciona control total sobre sus subredes y rangos de IP. Usted decide qué subredes crear, en las regiones que elija, con el rango de IP que especifique. Estos rangos de IP no se pueden superponer entre las subredes de una misma red.

Ahora bien, puede convertir redes de modo automático a redes en modo



personalizado para aprovechar el control que estas ofrecen. Sin embargo, la conversión funciona en un solo sentido, es decir, las redes en modo personalizado no se pueden transformar en redes de modo automático. Por lo tanto, revise con detenimiento las consideraciones sobre las redes de modo automático a fin de decidir qué tipo de red se ajusta a sus necesidades.

## Sistemas de aislamiento de redes



- A y B se pueden comunicar a través de IP internas, pese a que se encuentran en diferentes regiones.
- C y D se deben comunicar a través de IP externas, pese a que se encuentran en la misma región.

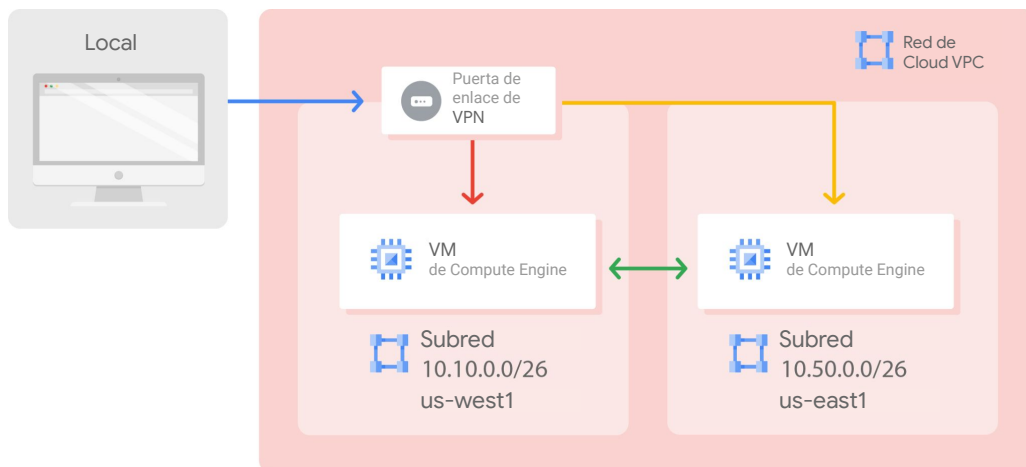
Google Cloud

En esta diapositiva, tenemos un ejemplo de un proyecto que contiene 5 redes. Todas ellas abarcan varias regiones del mundo, como puede ver en el lado derecho.

Cada red contiene máquinas virtuales independientes: A, B, C y D. Como las VMs A y B están en la misma red, la n° 1, pueden comunicarse mediante direcciones IP internas, pese a que están en regiones distintas. En términos simples, sus máquinas virtuales aprovechan la red global de fibra de Google, incluso si se encuentran en distintas partes del mundo. En cuanto al protocolo de configuración de red, las máquinas virtuales se muestran como si estuvieran en un mismo bastidor.

Sin embargo, las VMs C y D no están en la misma red. Por lo tanto, de forma predeterminada, deben comunicarse mediante direcciones IP externas, a pesar de que están en la misma región. El tráfico entre las VMs C y D no pasa por la Internet pública, sino que usa los routers perimetrales de Google. Esto tiene distintas consecuencias en la facturación y seguridad que exploraremos más adelante.

## La VPC de Google es global

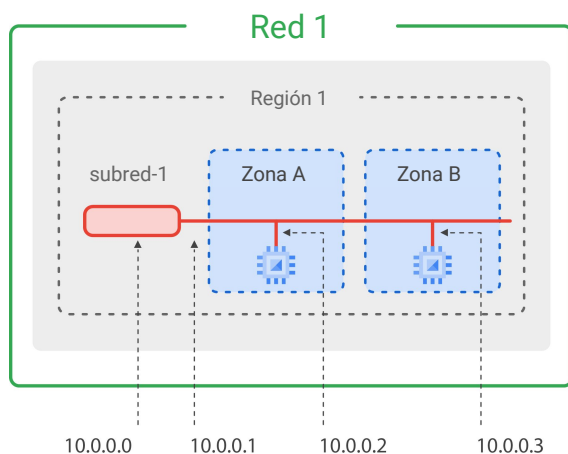


Google Cloud

Dado que las instancias de VM alojadas en una red de VPC se pueden comunicar de forma privada a escala global, una sola VPN puede conectar de forma segura su red local con la de Google Cloud, como se muestra en este diagrama. Aunque las dos instancias de VM están en regiones distintas (us-west1 y us-east1), aprovechan la red privada de Google para comunicarse entre ellas y con una red local mediante una puerta de enlace de VPN.

Esto permite reducir los costos y la complejidad de la administración de las redes.

## Las subredes atraviesan zonas



- Las VMs pueden estar en una misma subred, pero en zonas diferentes.
- Se puede aplicar la misma regla de firewall a ambas VMs.

Google Cloud

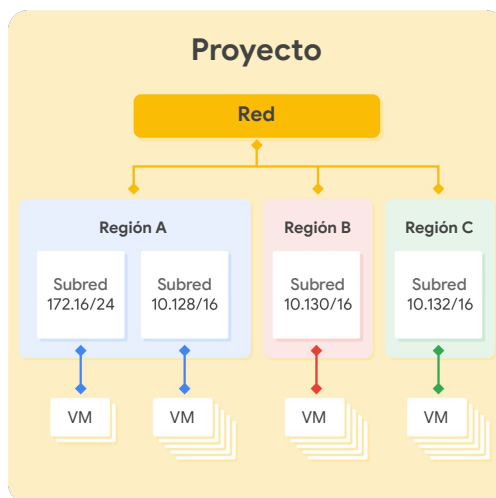
Mencioné que las subredes funcionan a escala regional. Como una región contiene varias zonas, las subredes pueden atravesarlas.

En esta diapositiva, se ve una región, la región 1, con dos zonas: A y B. Las subredes pueden extenderse entre estas zonas en la misma región, como la subred-1. La subred es solo un rango de direcciones IP, y usted podrá usar cualquier dirección IP dentro del rango. Tenga en cuenta que las dos primeras direcciones del rango, .0 y .1, se reservan para las puertas de enlace de la red y la subred, respectivamente. Por lo tanto, las primeras direcciones disponibles son .2 y .3, que se asignan a las instancias de VM. Las otras direcciones reservadas en cada subred son la penúltima dirección en el rango y la última, que está reservada como la dirección de “transmisión”. En resumen, cada subred tiene cuatro direcciones IP reservadas en su rango de IP principal.

A pesar de que las dos máquinas virtuales de este ejemplo se encuentran en zonas distintas, pueden comunicarse entre ellas con la misma dirección IP de la subred. Esto significa que se puede aplicar la misma regla de firewall a ambas VMs, aunque estén en zonas distintas.

## Expanda las subredes sin volver a crear instancias

- No se puede superponer con otras subredes.
- El rango de IP debe ser un bloque CIDR válido.
- Los rangos de IP de las nuevas subredes deben estar dentro de rangos de IP válidos.
- Se puede expandir, pero no reducir.
- El modo automático se puede expandir de /20 a /16.
- Evite las subredes grandes.



Google Cloud

En cuanto a las direcciones IP de una subred, puede usar las VPCs de Google Cloud para aumentar el espacio de dirección IP de cualquier subred sin cierres ni tiempo de inactividad de las cargas de trabajo.

En este diagrama, se muestra una red con subredes que tienen distintas máscaras, lo que permite que haya más instancias en algunas subredes que en otras. Esto le ofrece opciones de flexibilidad y crecimiento para satisfacer sus necesidades, pero también debe tener en cuenta los siguientes factores:

- La subred nueva no debe superponerse con otras de la misma red de VPC en ninguna región.
- Cada rango de IP para todas las subredes en una red de VPC debe ser un bloque CIDR válido.
- Además, los rangos de direcciones IP de las nuevas subredes son direcciones IP internas regionales y deben estar dentro de rangos de IP válidos.
  - Los rangos de subredes no pueden coincidir con un rango restringido, ni ser más estrechos ni más amplios que uno de estos rangos.
  - Los rangos de subredes no pueden abarcar un rango de RFC válido y un rango de direcciones IP públicas de uso privado.
  - Los rangos de subredes no pueden abarcar varios rangos de RFC.

- El rango de red nuevo debe ser más grande que el original, es decir, el valor de la longitud del prefijo debe ser un número más pequeño. En otras palabras, no puede deshacer una expansión.
- Las subredes de modo automático comienzan con un rango de IP /20. Se pueden expandir hasta un rango de IP máximo de /16. Como alternativa, puede convertir la subred de modo automático en una de modo personalizado a fin de aumentar aún más el rango de IP.
- Además, evite crear subredes grandes. Las subredes demasiado grandes tienen más posibilidades de generar colisiones del rango de CIDR cuando se usan interfaces de varias redes y el intercambio de tráfico entre redes de VPC, o cuando se configura una VPN o cualquier otra conexión a una red local. Por lo tanto, no debe escalar su subred más de lo que realmente necesita.

[Rangos de IP válidos: <https://cloud.google.com/vpc/docs/vpc#valid-ranges>]

# Demostración

---

## Expanda una subred



Ahora veremos cómo expandir una subred en Google Cloud.

Ya creé una subred personalizada con una máscara /29. Esta máscara proporciona 8 direcciones, pero, de ellas, 4 están reservadas por Google Cloud, lo que deja otras 4 para sus instancias de VM. Intentemos crear otra instancia de VM en esta subred.

[Demo]

Así de fácil es expandir una subred en Google Cloud sin interrupciones ni tiempo de inactividad en las cargas de trabajo.

# Temario

---

Nube privada virtual (VPC)

Proyectos, redes y subredes

Direcciones IP

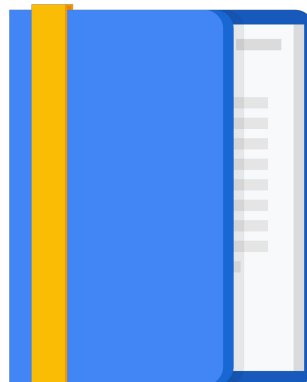
Rutas y reglas de firewall

Precios

Lab

Diseños comunes de redes

Lab



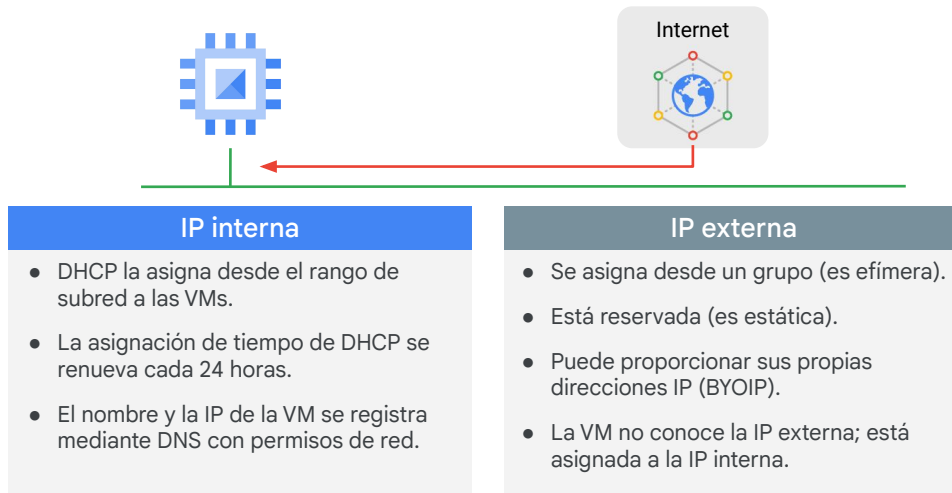
Ahora que explicamos las redes de Google Cloud de forma general, analicemos en detalle las direcciones IP.



## Las VMs deben tener direcciones IP internas y externas



Direcciones IP  
externas de la  
nube



En Google Cloud, cada máquina virtual puede tener dos direcciones IP asignadas. Una de ellas es interna y se asigna internamente con DHCP. Todas las VMs que se inicien y todos los servicios que dependan de una máquina virtual recibirán una dirección IP interna. Algunos ejemplos de estos servicios son App Engine y Google Kubernetes Engine, que analizaremos en otros cursos.

Cuando crea una VM en Google Cloud, se registra su nombre simbólico en un servicio de DNS interno que lo traduce a la dirección IP interna. El DNS está orientado a la red, por lo que puede traducir las URLs web y los nombres de las VMs de hosts de la misma red, pero no puede traducir los de las VMs de otras redes.

La otra dirección IP es la externa, pero es opcional. Puede asignar una dirección IP externa si su dispositivo o máquina son externos. La dirección IP externa se puede asignar desde un grupo, lo que la hará efímera. Otra opción es asignar una dirección IP externa reservada, lo que la convertirá en estática. Si reserva una dirección IP externa estática y no la asigna a un recurso, como una instancia de VM o una regla de reenvío, se le cobrará una tarifa más alta que por las otras direcciones IP externas estáticas y efímeras que estén en uso.

Puede usar sus propios prefijos de direcciones IP enrutables de forma pública como direcciones IP externas de Google Cloud y anunciarlos en Internet. A fin de ser apto,

debe ser propietario de un bloque de /24 o superior.

[\[https://cloud.google.com/compute/network-pricing#ipaddress\]](https://cloud.google.com/compute/network-pricing#ipaddress)

# Demostración

IP interna y externa



Se mencionó que las VMs pueden tener direcciones IP internas y externas.  
Explorémoslo en Cloud Console.

[Demo]

Esto demuestra que todas las VM necesitan una dirección IP interna, pero las externas son opcionales y efímeras de forma predeterminada.

# Las IP externas están asignadas a IP internas

<input type="checkbox"/> Nombre	Zona	Tipo de máquina	Recomendación	Usada por	IP interna	IP externa	Conexión
<input checked="" type="checkbox"/> instancia-1	us-east1-d	1 CPU virtual, 3,75 GB			10.142.0.2	104.196.149.82	SSH ▾ ⋮

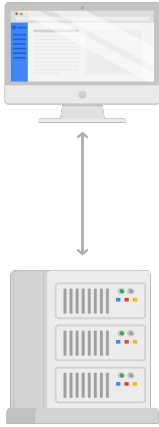
```
$ sudo /sbin/ifconfig
eth0
  Link encap:Ethernet HWaddr 42:01:0a:8e:00:02
  inet addr:10.142.0.2 Bcast:10.142.0.2 Mask:255.255.255.255
  UP BROADCAST RUNNING MULTICAST MTU:1460 Metric:1
  RX packets:397 errors:0 dropped:0 overruns:0 frame:0
  TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:66429 (64.8 KiB) TX bytes:41662 (40.6 KiB)

lo
  Link encap:Local Loopback
  inet addr:127.0.0.1 Mask:255.0.0.0
  inet6 addr: ::1/128 Scope:Host
  UP LOOPBACK RUNNING MTU:65536 Metric:1
  RX packets:0 errors:0 dropped:0 overruns:0 frame:0
  TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:0
  RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
```

Sin importar si usa una dirección IP externa efímera o estática, el SO de la VM no la conocerá. La dirección IP externa se asigna a la dirección interna de la VM de manera transparente por medio de la VPC. Con el fin de demostrarlo, ejecutaremos ifconfig en una VM de Google Cloud, que solo muestra una dirección IP interna.

Con el fin de analizar este aspecto en más detalle, veamos la resolución de DNS para direcciones internas y externas.

## Resolución de DNS para direcciones internas



Cada instancia tiene un nombre de host que se puede resolver en una dirección IP interna:

- El nombre del host es igual al nombre de la instancia.
- FQDN es [hostname].[zone].c.[project-id].internal

Ejemplo: my-server.us-central1-a.c.guestbook-151617.internal

La resolución de nombres se controla con una resolución de DNS interna:

- Se entrega como parte de Compute Engine (169.254.169.254).
- DHCP lo configura para el uso en la instancia.
- Entrega respuestas para direcciones internas y externas.

Comencemos por las direcciones internas.

Cada instancia tiene un nombre de host que se puede resolver en una dirección IP interna. El nombre del host es igual al nombre de la instancia. También hay un nombre de dominio interno completamente calificado (o FQDN) para una instancia que usa el formato que se muestra en la diapositiva.

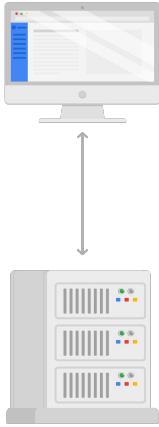
Si borra una instancia y vuelve a crearla, es posible que cambie la dirección IP interna. Esto puede interrumpir las conexiones de otros recursos de Compute Engine, que deberán tener la dirección IP nueva para conectarse nuevamente. Sin embargo, el nombre del DNS siempre se dirige a una instancia específica, sin importar cuál sea la dirección IP interna.

Cada instancia tiene un servidor de metadatos que también actúa como agente de resolución de DNS para esa instancia. El servidor de metadatos controla todas las consultas de DNS de los recursos de la red local y enruta todas las demás consultas a los servidores DNS públicos de Google para obtener una resolución de nombre pública. Anteriormente, mencioné que las instancias no conocen las direcciones IP externas que se les asignan. En cambio, la red almacena una tabla de consulta que combina las direcciones IP externas con las internas de las instancias relevantes.

Para obtener más información, incluida la manera de configurar su propio agente de resolución en instancias, consulte la sección de vínculos de este video.

[\[https://cloud.google.com/compute/docs/vpc/internal-dns\]](https://cloud.google.com/compute/docs/vpc/internal-dns)

## Resolución de DNS para direcciones internas



- Las instancias con direcciones IP externas pueden permitir conexiones desde hosts fuera del proyecto.
  - Los usuarios se conectan directamente con direcciones IP externas.
  - Los administradores también pueden publicar registros DNS públicos que se dirigen a la instancia.
    - Los registros DNS públicos no se publican automáticamente.
- Los registros DNS para direcciones externas se pueden publicar con servidores DNS existentes (fuera de Google Cloud).
- Las zonas del DNS se pueden alojar en Cloud DNS.

Ahora analicemos las direcciones externas.

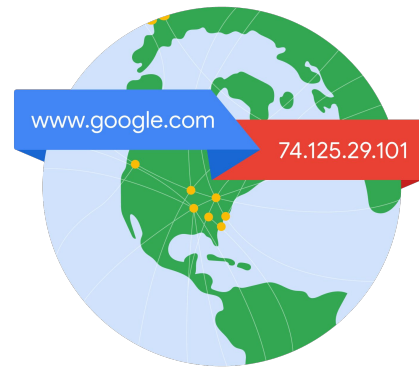
Las instancias con direcciones IP externas pueden permitir conexiones desde hosts fuera del proyecto. Los usuarios también pueden hacerlo de forma directa con la dirección IP externa. Los registros DNS públicos que se dirigen a las instancias no se publican automáticamente. Sin embargo, los administradores pueden publicarlos con los servidores DNS existentes.

Los servidores de nombres de dominio se pueden alojar en Google Cloud con Cloud DNS. Este es un servicio administrado que definitivamente vale la pena considerar, así que lo analizaremos en profundidad.

# Aloje zonas del DNS con Cloud DNS



- Servicio DNS de Google
- Convierte los nombres de dominio en direcciones IP
- Latencia baja
- Alta disponibilidad (ANS de 100% de tiempo de actividad)
- Crea y actualiza millones de registros DNS
- IU, línea de comandos o API



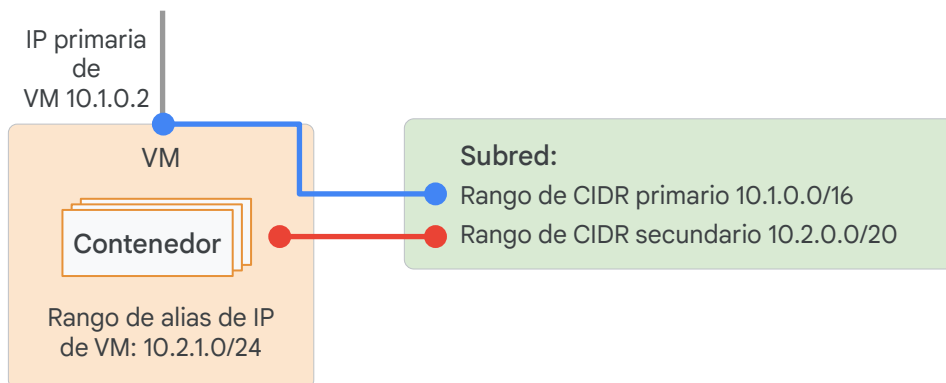
Cloud DNS es un servicio de sistema de nombres de dominio (DNS) autorizado, escalable, confiable y administrado que se ejecuta en la misma infraestructura que Google. Cloud DNS transforma las solicitudes de los nombres de dominio, como google.com, en direcciones IP.

Cloud DNS usa la red global de Google de los servidores de nombres de Anycast para entregar sus zonas del DNS desde ubicaciones redundantes en todo el mundo, lo que permite ofrecer una latencia más baja y alta disponibilidad a sus usuarios. La alta disponibilidad es muy importante porque, si no puede buscar el nombre de un dominio, es posible que no tenga conexión a Internet. Por eso, Google Cloud ofrece un Acuerdo de Nivel de Servicio (ANS) con 100% de tiempo de actividad para dominios configurados en Cloud DNS. Si desea obtener más información sobre el ANS, consulte la sección de vínculos de este video. [<https://cloud.google.com/dns/sla>]

Con Cloud DNS, puede crear y actualizar millones de registros DNS sin preocuparse de administrar sus propios servidores DNS ni software. En lugar de ello, puede usar una interfaz de usuario simple, una interfaz de línea de comandos o una API. Para obtener más información sobre Cloud DNS, consulte la sección de vínculos de este video. [<https://cloud.google.com/dns/docs/>]



## Asigne un rango de direcciones IP como alias de una interfaz de red de VM que usa rangos de alias de IP



Otra función de las redes de Google Cloud son los rangos de alias de IP.

Estos le permiten asignar un rango de direcciones IP internas como un alias a una interfaz de red de una máquina virtual. Esto es útil si tiene varios servicios ejecutándose en una VM y desea asignar una dirección IP a cada uno.

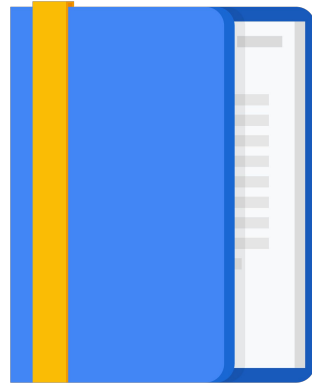
En términos sencillos, puede configurar varias direcciones IP que representen los contenedores o las aplicaciones que se alojan en una VM, sin necesidad de definir una interfaz de red por separado. Solo debe obtener el rango de alias de IP de los rangos CIDR principales o secundarios de la subred local. En este diagrama, se proporciona una ilustración básica de los rangos de CIDR principales y secundarios, y de los rangos de alias de IP de la VM.

Para obtener más información sobre los rangos de alias de IP, consulte la sección de vínculos de este video. [<https://cloud.google.com/compute/docs/alias-ip/>]

# Temario

---

- Nube privada virtual (VPC)
- Proyectos, redes y subredes
- Direcciones IP
- Rutas y reglas de firewall
- Precios
- Lab
- Diseños comunes de redes
- Lab



Hasta ahora, aprendió sobre los proyectos, las redes, las subredes y las direcciones IP. Usemos esa información para comprender de qué manera Google Cloud enruta el tráfico.

# Una ruta es una asignación de un rango de IP a un destino



Cada red tiene los siguientes elementos:

- Rutas que permiten a las instancias de una red enviarse tráfico directamente entre ellas
- Una ruta predeterminada que dirige los paquetes a destinos que están fuera de la red

*Las reglas de firewall también deben autorizar los paquetes.*

De forma predeterminada, cada red tiene rutas que permiten a las instancias de una red enviarse el tráfico directamente entre ellas, incluso entre subredes. Además, cada red tiene una ruta predeterminada que dirige los paquetes a destinos fuera de ella.

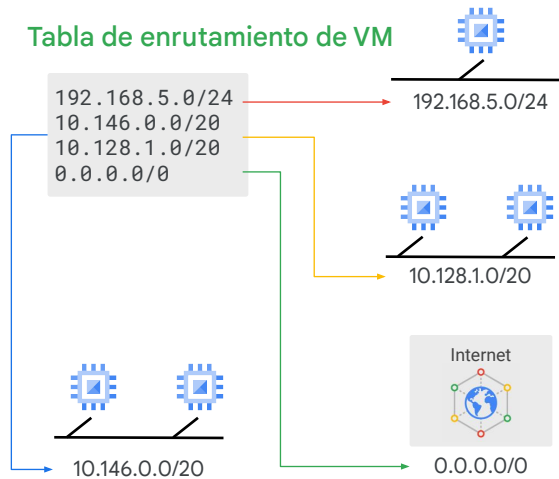
A pesar de que las rutas satisfacen la mayor parte de sus necesidades comunes de enrutamiento, también puede crear rutas especiales que anulen a las otras.

El solo hecho de crear una ruta no garantiza que sus paquetes se recibirán en el siguiente salto que indique. Las reglas de firewall también deben autorizar los paquetes.

La red predeterminada tiene reglas de firewall preconfiguradas que permiten que todas las instancias de la red se comuniquen entre ellas. Las redes creadas de forma manual no tienen esas reglas, por lo que usted debe crearlas, tal como lo verá en el primer lab.

## Las rutas asignan tráfico a redes de destino

- Se aplican al tráfico que sale de una VM.
- Desvían tráfico a la ruta más específica.
- Se crean cuando se crea una subred.
- Habilitan la comunicación entre VMs en la misma red.
- El destino está en notación CIDR.
- El tráfico solo se entrega si también coincide con una regla de firewall.

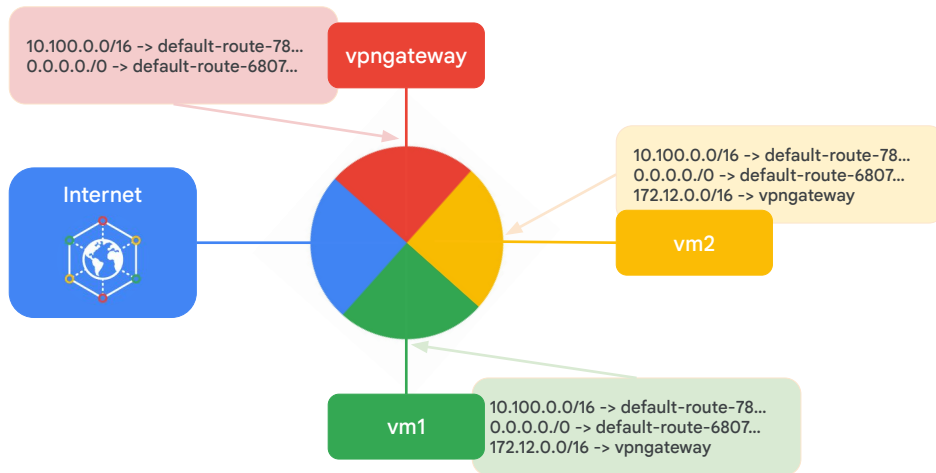


Las rutas hacen coincidir los paquetes según su dirección IP de destino. Sin embargo, no se permitirá el tráfico que no coincida con una regla de firewall específica.

Las rutas se crean cuando se crean las redes, lo que permite la entrada de tráfico desde “cualquier lugar”. También se crean rutas cuando se crean subredes. Esto permite que las VMs de una misma red se comuniquen entre ellas.

En esta diapositiva, se muestra una tabla de enrutamiento simplificada, pero veámosla con más detalle.

## Tablas de enrutamiento de instancias



Todas las rutas de la colección Rutas pueden aplicarse a una o más instancias. Las rutas se aplican a una instancia si coinciden la red y las etiquetas de la instancia. Si la red coincide y no se especificaron etiquetas de instancias, se aplica la ruta a todas las instancias de la red. Luego, Compute Engine usa la colección Rutas a fin de crear tablas de enrutamiento de solo lectura para cada instancia.

En este diagrama, se muestra un router virtual con alta escalabilidad en el centro de cada red. Cada instancia de máquina virtual de la red está conectada directamente con el router. Además, todos los paquetes que salen de una instancia de máquina virtual se administran en esta capa antes de enviarlos al siguiente salto. Para elegir el siguiente salto de un paquete, el router de la red virtual consulta la tabla de enrutamiento de esa instancia.

# Las reglas de firewall protegen sus instancias de VM de las conexiones no autorizadas



- Las redes de VPC funcionan como un firewall distribuido.
- Las reglas de firewall se aplican a toda la red.
- Las conexiones se *permiten* o se *rechazan* a nivel de cada instancia.
- Las reglas de firewall son reglas con estado.
- Existen reglas implícitas para *denegar todas las entradas* y *permitir todas las salidas*.

Las reglas de firewall de Google Cloud protegen sus instancias de máquinas virtuales de las conexiones no autorizadas entrantes y salientes, conocidas como de entrada y salida, respectivamente. En términos sencillos, cada red de VPC funciona como un firewall distribuido.

Aunque las reglas de firewall se aplican a toda la red, las conexiones se permiten o rechazan a nivel de cada instancia. Puede pensar que el firewall existe no solo entre sus instancias y otras redes, sino también entre instancias individuales dentro de la misma red.

Las reglas de firewall de Google Cloud tienen estado. Esto significa que, si se permite una conexión entre un origen y un objetivo o entre un objetivo y un destino, se permitirá todo el tráfico posterior en cualquier dirección. Es decir, las reglas de firewall permiten la comunicación bidireccional una vez que se establece una sesión.

Además, si por algún motivo se borran todas las reglas de firewall de una red, aún hay una regla de entrada implícita llamada “Rechazar todo” y otra de salida llamada “Permitir todo” en la red.

## Las rutas asignan tráfico a redes de destino

Parámetro	Detalles
direction	Las conexiones de entrada se comparan solo con las reglas de ingress.
	Las conexiones de salida se comparan solo con las reglas de egress.
source o destination	Para la dirección ingress, sources se puede especificar como parte de la regla con direcciones IP, etiquetas de origen o una cuenta de servicio de origen.
	Para la dirección egress, destinations se puede especificar como parte de una regla con uno o más rangos de direcciones IP.
protocol y port	Cualquier regla se puede restringir para que se aplique solo a protocolos o solo a combinaciones específicas de protocolos y puertos.
action	Permite o rechaza los paquetes que coincidan con la dirección, el protocolo, el puerto y el origen o el destino de la regla.
priority	Establece el orden en que se evalúan las reglas; se aplica la primera regla que coincide.
rule assignment	Todas las reglas se asignan a todas las instancias, pero puede asignar algunas de ellas solo a ciertas instancias.

Puede indicar la configuración que desea para su firewall como un conjunto de reglas. Desde una perspectiva conceptual, una regla de firewall se compone de los siguientes parámetros:

- La **dirección** (direction) de la regla. Las conexiones de entrada se comparan solo con las reglas de entrada, mientras que las conexiones de salida se comparan con las reglas de salida.
- El **origen** (source) de la conexión de los paquetes de entrada o el **destino** (destination) de la conexión de los paquetes de salida.
- El **protocolo** (protocol) y el **puerto** (port) de la conexión, en los que se pueden restringir las reglas para que se apliquen solo a protocolos específicos o solo a combinaciones específicas de protocolos y puertos.
- La **acción** (action) de las reglas, que es permitir o rechazar los paquetes que coincidan con la dirección, el protocolo, el puerto y el origen o el destino de la regla.
- La **prioridad** (priority) de las reglas, que se encarga del orden en que estas se evalúan. Se aplica la primera regla coincidente.
- La **asignación de la regla** (rule assignment). De forma predeterminada, todas las reglas se asignan a todas las instancias, pero puede asignar algunas de ellas solo a ciertas instancias.

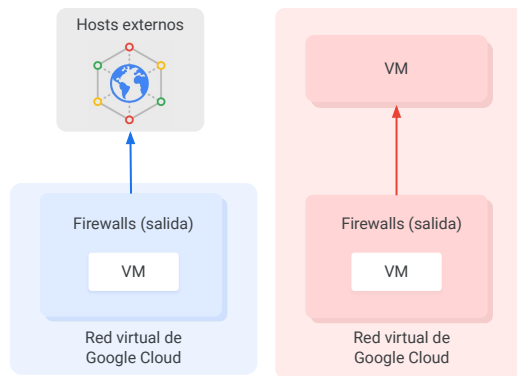
Para obtener más información sobre los componentes de las reglas de firewall, consulte la sección de vínculos de este video.

[\[https://cloud.google.com/compute/docs/vpc/firewalls#firewall\\_rule\\_components\]](https://cloud.google.com/compute/docs/vpc/firewalls#firewall_rule_components)

Analicemos algunos casos de uso del firewall de Google Cloud para salidas y entradas.



## Caso de uso del firewall de Google Cloud: salida



### Condiciones:

- Rangos CIDR de destino
- Protocolos
- Puertos

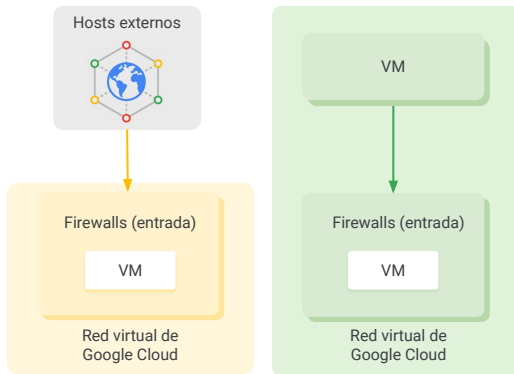
### Acción:

- allow: autoriza la conexión de salida coincidente
- deny: bloquea la conexión de salida coincidente

Las reglas de firewall de salida controlan las conexiones salientes que se originan dentro de la red de Google Cloud. Las reglas **allow** de salida permiten las conexiones salientes que coinciden con las direcciones IP, el protocolo y los puertos específicos. Las reglas **deny** de salida evitan que las instancias inicien conexiones que coincidan con combinaciones de rangos de IP, puertos o protocolos no permitidos.

En el caso de las reglas de firewall de salida, los destinos a los que se aplica la regla podrían indicarse con los rangos de IP de CIDR. Específicamente, puede usar rangos de destino para protegerse contra las conexiones no deseadas que inicie una instancia de VM hacia un host externo, tal como se muestra a la izquierda. También puede usar los rangos de destino para evitar las conexiones no deseadas desde instancias de VM internas a un rango de CIDR específico de Google Cloud. Esto se demuestra en el centro, en el que una VM de una subred específica intenta conectarse de forma inapropiada a otra de la misma red.

## Caso de uso del firewall de Google Cloud: entrada



### Condiciones:

- Rangos de CIDR de origen
- Protocolos
- Puertos

### Acción:

- allow: autoriza la conexión de entrada coincidente
- deny: bloquea la conexión de entrada coincidente

Las reglas de firewall de entrada lo protegen contra las conexiones entrantes a la instancia desde cualquier origen. Las reglas **allow** de entrada permiten que se conecten direcciones IP, puertos y protocolos específicos. El firewall evita que las instancias reciban conexiones en puertos o protocolos no permitidos. Se pueden restringir las reglas para que se apliquen solo a algunos orígenes.

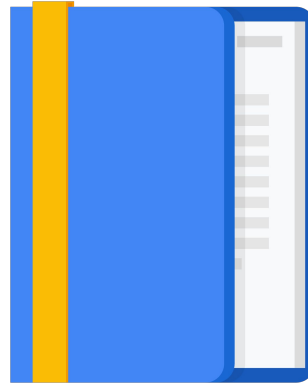
Los rangos de CIDR de origen pueden usarse para proteger una instancia de las conexiones no deseadas que provengan de redes externas o de rangos de IP de Google Cloud.

En este diagrama, se muestra una VM que recibe una conexión desde una dirección externa y otra que recibe una conexión de otra VM desde la misma red. A fin de controlar las conexiones de entrada desde una instancia de VM, cree condiciones para las conexiones entrantes con rangos de CIDR de origen, protocolos o puertos.

# Temario

---

- Nube privada virtual (VPC)
- Proyectos, redes y subredes
- Direcciones IP
- Rutas y reglas de firewall
- Precios**
- Lab
- Diseños comunes de redes
- Lab



Antes de poner en práctica lo que aprendió, hablemos sobre los precios de red. Es importante que comprenda las circunstancias en las que se le factura por la red de Google Cloud.

## Precios de red (sujetos a cambios)

Tipo de tráfico	Precio (USD)
Entrada	Sin cargo
Salida a la misma zona (dirección IP interna)	Sin cargo
Salida a productos de Google (YouTube, Maps, Drive)	Sin cargo
Salida a un servicio distinto de Google Cloud (dentro de la misma región; con excepciones)	Sin cargo
Salida entre zonas de la misma región (por GB)	\$0.01
Salida a la misma zona (dirección IP externa, por GB)	\$0.01
Salida entre regiones dentro de Canadá y EE.UU. (por GB)	\$0.01
Salida entre regiones, sin incluir el tráfico entre regiones de EE.UU.	Depende de la región

Esta tabla forma parte de la documentación de Compute Engine y, en ella, se indican los precios de cada tipo de tráfico.

En primer lugar, no se cobra por la entrada o el tráfico que llega a la red de Google Cloud, a menos que exista un recurso, como un balanceador de cargas, que esté procesando el tráfico de entrada. Se cobran las respuestas a solicitudes, ya que cuentan como tráfico de salida.

En el resto de la tabla, se muestra la salida o el tráfico que sale de una máquina virtual. El tráfico de salida a la misma zona no se cobra, siempre que esa salida sea por medio de la dirección IP interna de una instancia. Tampoco se cobran el tráfico de salida a productos de Google, como YouTube, Maps o Drive, ni el tráfico a un servicio distinto de Google Cloud dentro de la misma región.

Sin embargo, sí se cobra la salida entre zonas de la misma región, la salida dentro de una zona si el tráfico ocurre por medio de la dirección IP externa de una instancia y la salida entre regiones.

En cuanto a la diferencia en el tráfico de salida a la misma zona, Compute Engine no puede determinar la zona de una máquina virtual a través de la dirección IP externa. Por lo tanto, este tráfico se considera de salida entre zonas de la misma región.

Además, existen algunas excepciones y los precios siempre pueden cambiar, por lo que recomendamos revisar la documentación en la sección de vínculos de este video [<https://cloud.google.com/compute/network-pricing>]

## Precios de dirección IP externa (us-central1)

(Sujetos a cambios)

Tipo	Precio/hora (USD)
Dirección IP estática (asignada, pero sin usar)	\$0.010
Direcciones IP estáticas y efímeras utilizadas en instancias de VM <b>estándar</b>	\$0.004
Direcciones IP estáticas y efímeras en uso en instancias de VM <b>interrumpibles</b>	\$0.002
Direcciones IP estáticas y efímeras vinculadas a reglas de reenvío	Sin cargo

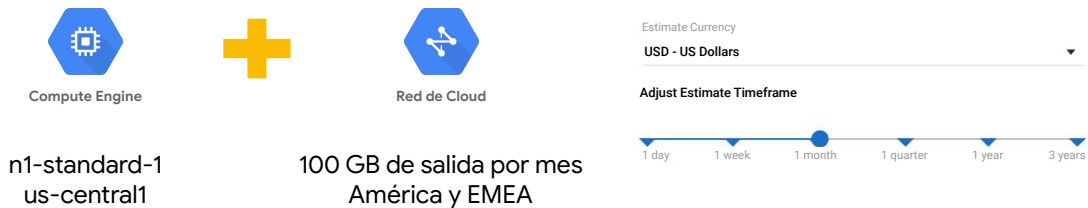
Se le cobra por direcciones IP externas estáticas y efímeras. En esta tabla, se muestran los precios de dirección IP externa para us-central1 cuando se grabó esta presentación.

Como seguramente notó, si reserva una dirección IP externa estática y no la asigna a un recurso, como una instancia de VM o una regla de reenvío, se le cobrará una tarifa más alta que por las otras direcciones IP externas estáticas y efímeras que estén en uso. Además, las direcciones IP externas en VM interrumpibles tiene un precio inferior al de las instancias de VM estándar.

Recuerde que los precios siempre pueden cambiar, por lo que recomendamos consultar el vínculo a la documentación en las diapositivas.

[\[https://cloud.google.com/compute/network-pricing#ipaddress\]](https://cloud.google.com/compute/network-pricing#ipaddress)

## Estime los costos con la calculadora de precios de Google Cloud



Se recomienda usar la calculadora de precios de Google Cloud para estimar el costo de un conjunto de recursos, ya que cada servicio tiene su propio modelo de precios. La calculadora de precios es una herramienta basada en la Web que puede usar para especificar el consumo esperado de ciertos servicios y recursos, y así obtener un costo estimado.

Por ejemplo, puede especificar un tipo de instancia en particular en una región específica y 100 GB de tráfico de salida mensual a América y EMEA. Luego, la calculadora de precios le mostrará el costo total estimado. Puede ajustar la moneda y el período necesario para satisfacer sus necesidades y, cuando termine, puede enviar la estimación por correo electrónico o guardarla en una URL específica con el fin de consultarla en el futuro.

Para utilizar la calculadora de precios ahora mismo, consulte la sección de vínculos de este video. [<https://cloud.google.com/products/calculator/>]

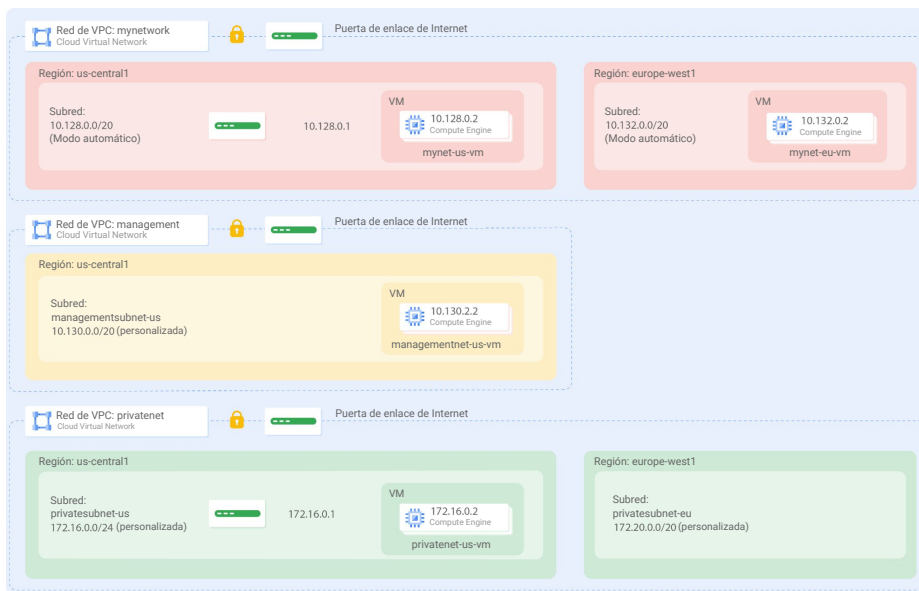
# Lab

---

## Redes de VPC

Apliquemos en un lab algunas de las funciones de red que acabamos de analizar.





En este lab, creará una red de VPC de modo automático con reglas de firewall y dos instancias de VM. Luego, convertirá la red de modo automático en una red de modo personalizado y creará otras redes de este tipo, como se muestra en el diagrama de red. También explorará la conectividad entre las redes.

# Revisión del lab

---

## Redes de VPC

En este lab, exploró la red predeterminada y estableció que no puede crear instancias de VM sin una red de VPC. Por lo tanto, creó una nueva red de VPC de modo automático con subredes, rutas, reglas de firewall y dos instancias de VM, y probó la conectividad para esas instancias. Dado que no se recomiendan las redes de modo automático para procesos de producción, convirtió la red de modo automático en una red de modo personalizado.

Luego, creó dos redes adicionales de VPC de modo personalizado con instancias de VM y reglas de firewall mediante Google Cloud Console y la línea de comandos de gcloud. Por último, probó la conectividad entre redes de VPC, que funcionó tras hacer ping a direcciones IP externas, pero no a IP internas.

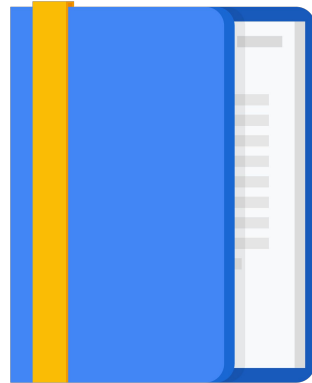
De forma predeterminada, las redes de VPC son dominios de redes privadas aisladas. Por lo tanto, no se permite la comunicación de direcciones IP internas entre redes, a menos que configure mecanismos como una conexión de VPN o el intercambio de tráfico de VPC.

Puede continuar con un recorrido por el lab, pero recuerde que la interfaz de usuario de Google Cloud puede cambiar, por lo que su entorno podría ser un poco diferente.

# Temario

---

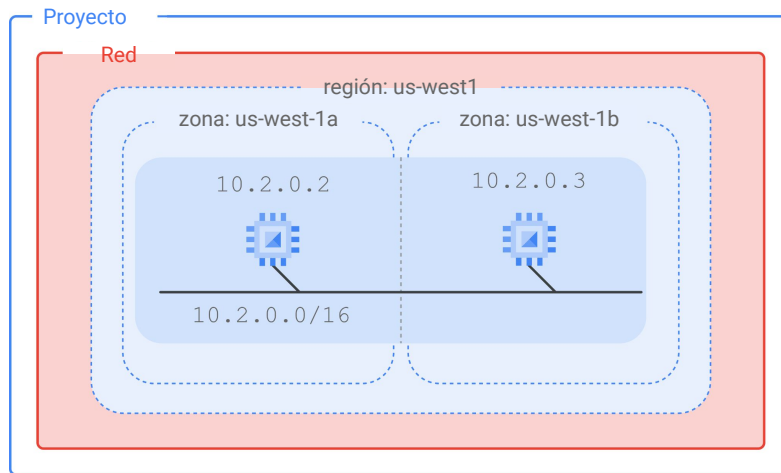
- Nube privada virtual (VPC)
- Proyectos, redes y subredes
- Direcciones IP
- Rutas y reglas de firewall
- Precios
- Lab
- Diseños comunes de redes**
- Lab



Usemos lo que aprendimos hasta ahora y analicemos diseños de red comunes.

“Común” es un término bastante relativo. Aunque podríamos pasar todo el día hablando de los diseños de red, elegimos un conjunto que se relaciona mejor con este módulo.

## Disponibilidad aumentada con varias zonas

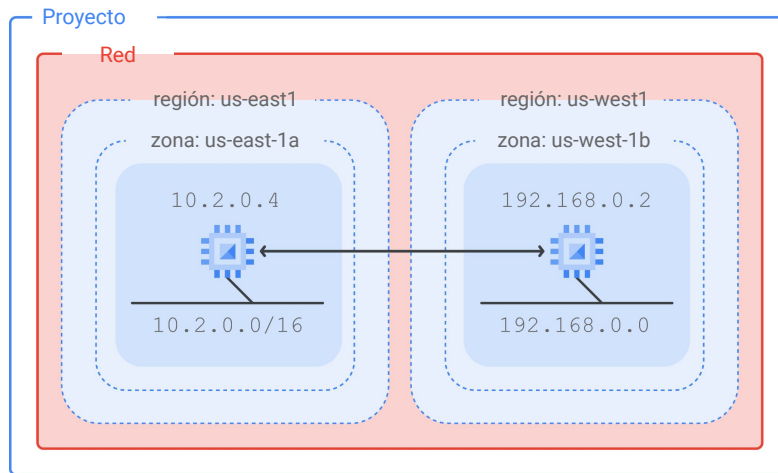


Para comenzar, veamos la disponibilidad.

Si su aplicación necesita más disponibilidad, puede colocar dos máquinas virtuales en múltiples zonas (pero dentro de la misma subred), como se muestra en esta diapositiva. Con una sola subred, puede crear una regla de firewall para la subred `10.2.0.0/16`.

Por lo tanto, si asigna las VMs en una sola subred en zonas separadas, obtendrá disponibilidad mejorada sin la complejidad de seguridad adicional. Un grupo de instancias administrado regional contiene instancias de múltiples zonas en la misma región, que ofrece mayor disponibilidad.

## Globalización con varias regiones



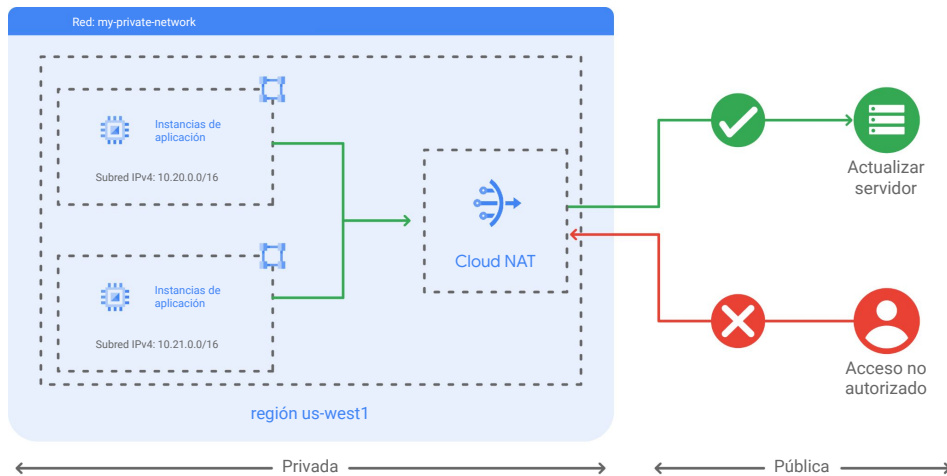
A continuación, analicemos la globalización.

En el diseño anterior, colocamos recursos en zonas diferentes dentro de una sola región, lo que ofrece aislamiento de muchos tipos de fallas de infraestructura, hardware y software. Ubicar recursos en diferentes regiones como se muestra en esta diapositiva proporciona un mayor grado de independencia ante fallas. Esto le permite diseñar sistemas sólidos mediante la distribución de recursos en diferentes dominios con fallas.

Cuando usa un balanceador de cargas global, como el balanceador de cargas de HTTP, puede enrutar el tráfico a la región más cercana al usuario. Esto puede generar mejor latencia para los usuarios y costos más bajos de tráfico de red en su proyecto.

Exploraremos ambos grupos de instancias administrados y el balanceador de cargas más adelante en la serie de cursos.

## Cloud NAT proporciona acceso a Internet para instancias privadas

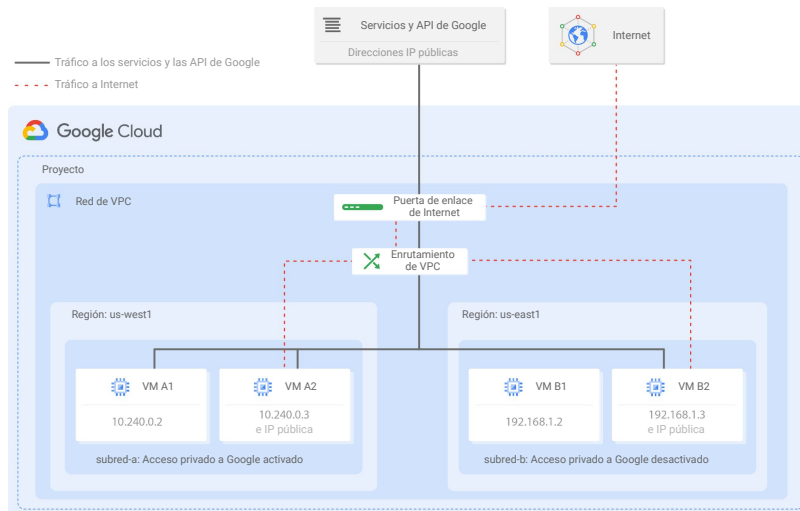


Como práctica recomendada de seguridad general, sugerimos que, cuando sea posible, use solo direcciones IP internas asignadas a sus instancias de VM.

Cloud NAT es el servicio de traducción de direcciones de red de Google. Le permite aprovisionar sus instancias de aplicaciones sin direcciones IP públicas y, al mismo tiempo, les permite acceder a Internet de forma eficaz y controlada. Esto significa que sus instancias privadas pueden acceder a Internet para obtener actualizaciones, parches, administración de configuración y más.

En este diagrama, Cloud NAT permite que dos instancias privadas accedan a un servidor de actualización en Internet, que se denomina NAT de salida. Sin embargo, Cloud NAT no implementa NAT de salida. En otras palabras, los hosts fuera de su red de VPC no pueden acceder directamente a las instancias privadas detrás de la puerta de enlace de Cloud NAT. Esto ayuda a mantener sus redes de VPC aisladas y seguras.

## Acceso privado a los servicios y las API de Google



Del mismo modo, debe habilitar el Acceso privado a Google a fin de permitir que las instancias de VM que solo tienen direcciones IP internas lleguen a direcciones IP externas de los servicios y las API de Google. Por ejemplo, si su instancia de VM necesita acceder a un bucket de Cloud Storage, debe habilitar el Acceso privado a Google.

Debe habilitar el Acceso privado a Google en cada subred. Como puede ver en este diagrama, el Acceso privado a Google está habilitado en la subred-a e inhabilitado en la subred-b. Esto permite que la VM A1 acceda a los servicios y las API de Google, aunque no tenga una dirección IP externa.

El Acceso privado a Google no influye en las instancias que tienen direcciones IP externas. Por eso, las VMs A2 y B2 pueden acceder a los servicios y las API de Google. La única VM que no puede acceder a esos servicios y API es la VM B1. Esta no tiene una dirección IP pública y es una subred en la que está inhabilitado el Acceso privado a Google.

# Lab

---

Implemente el  
Acceso privado a Google y  
Cloud NAT

Philipp Maier

Apliquemos los conocimientos que acabamos de adquirir.

En este lab, implementará el Acceso privado a Google y Cloud NAT en una instancia de VM que no tenga una dirección IP externa. Luego, verificará el acceso a las direcciones IP públicas de los servicios y las API de Google, y otras conexiones a Internet.



# Revisión del lab

---

Implemente el  
Acceso privado a Google y  
Cloud NAT

Philipp Maier

En este lab, creó una instancia sin una dirección IP externa y accedió a ella mediante Cloud IAP. Luego, habilitó el Acceso privado a Google, configuró una puerta de enlace de NAT y verificó que vm-internal pudiera acceder a los servicios y las API de Google y a otras direcciones IP públicas.

Las instancias de VM que no tienen direcciones IP externas están aisladas de las redes externas. Con Cloud NAT, estas instancias pueden acceder a Internet para obtener actualizaciones y parches y, en algunos casos, inicializaciones. Por ser un servicio administrado, Cloud NAT proporciona alta disponibilidad sin administración ni intervención por parte del usuario.

Lo guiaremos a través de este lab. Ahora, recuerde que la interfaz de usuario de Google Cloud puede cambiar, por lo que su entorno podría ser un poco diferente.

# Repaso

---

## Redes virtuales

En este módulo, presentamos una descripción general de la nube privada virtual de Google. Vimos los distintos componentes de las VPC, como los proyectos, las redes, las direcciones IP, las rutas y las reglas de firewall. También brindamos una descripción general breve de la forma en que las opciones de diseño de la red pueden afectar la facturación.

Luego, aplicamos los diferentes conceptos en un lab minucioso.

A continuación, observamos diseños de red comunes y pudimos implementar el Acceso privado a Google y Cloud NAT en un lab.

Ahora que tiene una perspectiva sólida de la forma en que Google Cloud implementó las redes, aprenderemos sobre otros servicios. Hablemos sobre Compute Engine, que ofrece máquinas virtuales escalables y de alto rendimiento.