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.

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

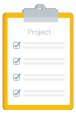
Con Google Cloud, puede aprovisionar sus recursos del servicio, conectarlos a otros y aislarlos en una nube privada virtual. También puede definir políticas detalladas de red en Google Cloud, y entre Google Cloud y otros entornos locales o nubes públicas. En términos simples, VPC es un conjunto integral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

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:

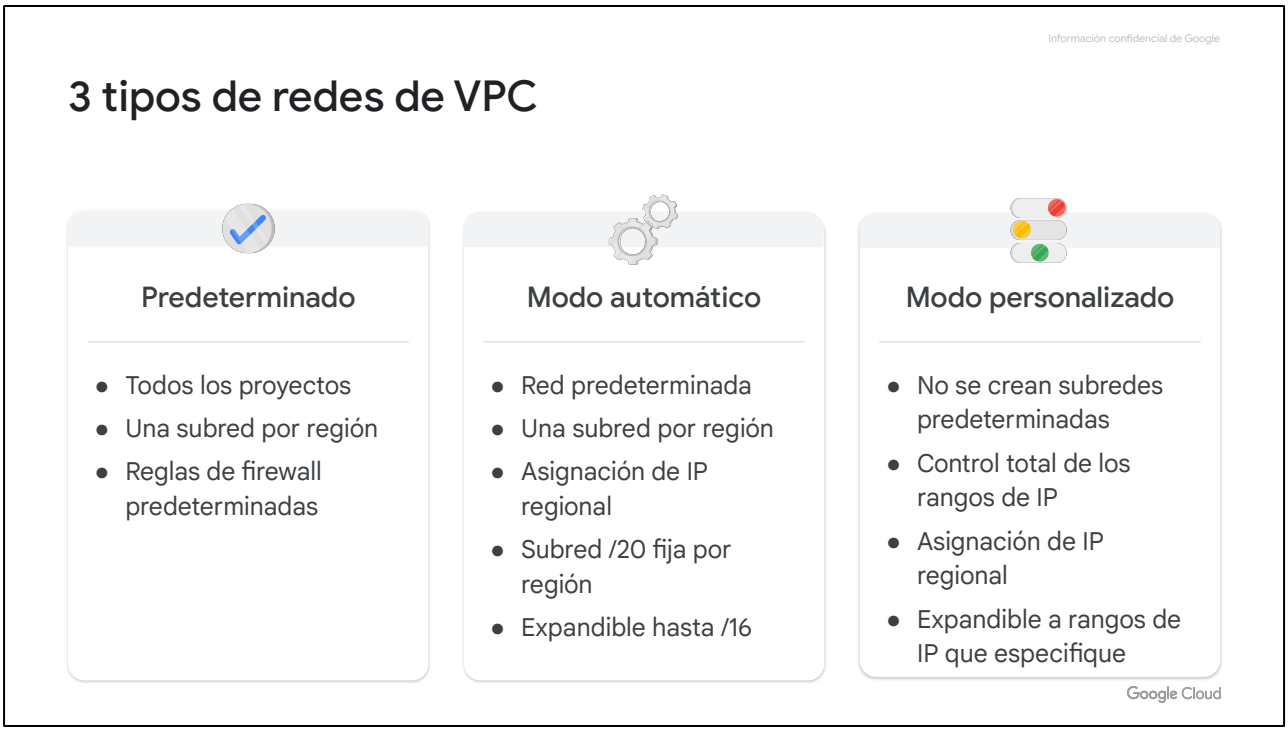
- No tienen rangos de direcciones IP.
- Son globales y abarcan todas las regiones disponibles.
- Contienen subredes.
- Están disponibles como predeterminadas, automáticas o personalizadas.

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.



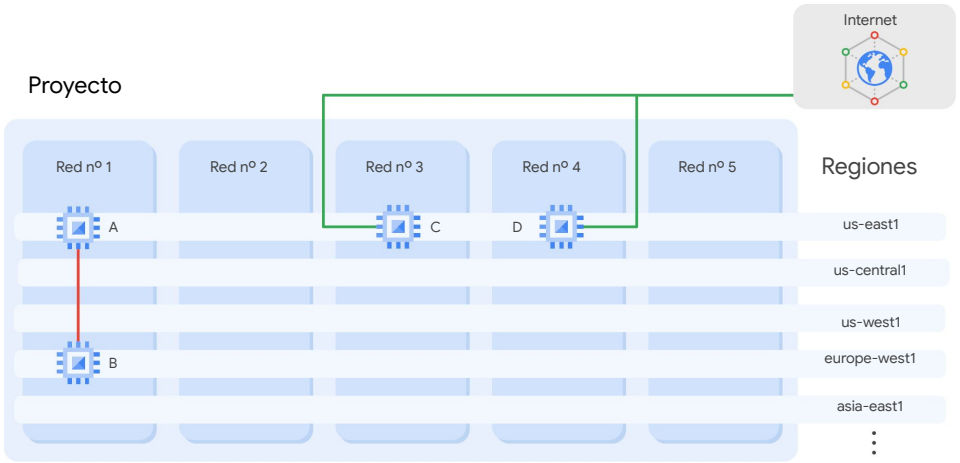
Todos los proyectos cuentan con una red de VPC predeterminada, que tiene subredes y reglas de firewall predefinidas. Específicamente, se asigna una subred a cada región con bloques CIDR no superpuestos y reglas de firewall que permiten tráfico de entrada de ICMP, RDP y SSH desde cualquier lugar, además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

Sistemas de aislamiento de redes



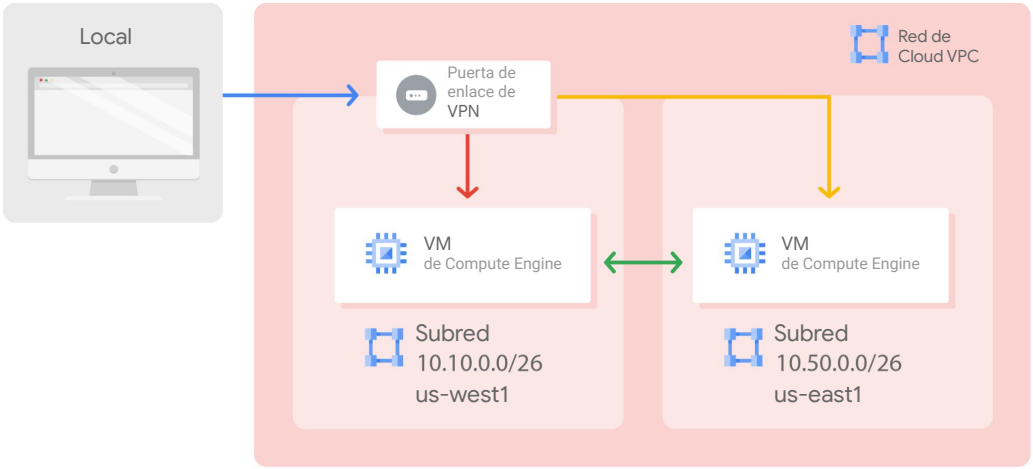
- **A** y **B** se pueden comunicar a través de IP internas, *pese a que se encuentran en diferentes regiones.*
- **C** y **D** se deben comunicar a través de IP externas, *pese a que se encuentran en la misma región.*

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 nº 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.

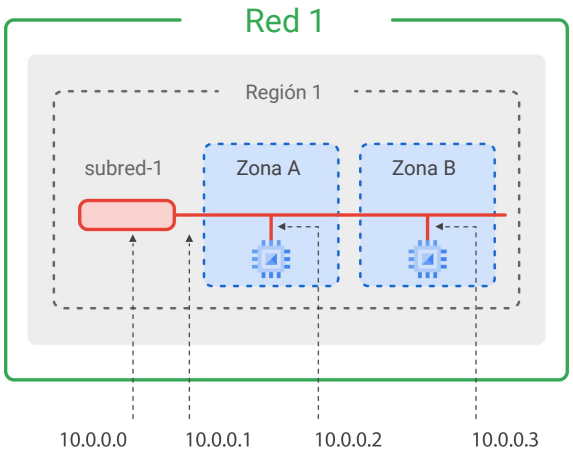
Sin embargo, las VMs C y D no están en la misma red. Por lo tanto, de forma predeterminada, deben comunicarse mediante direcciones IP externas, a pesar de que están en la misma región. El tráfico entre las VMs C y D no pasa por la Internet pública, sino que usa los routers perimetrales de Google. Esto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

La VPC de Google es global



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.

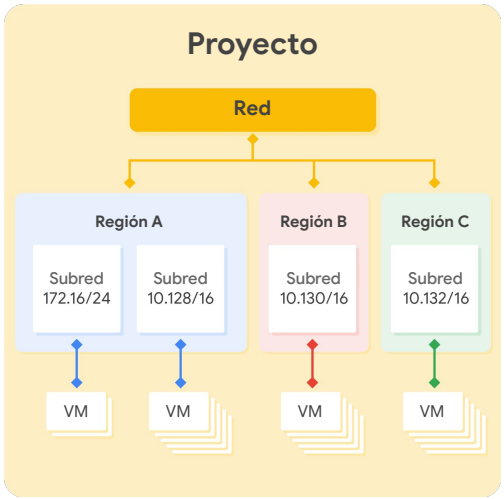
Mencioné que las subredes funcionan a escala regional. Como una región contiene varias zonas, las subredes pueden atravesarlas.

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

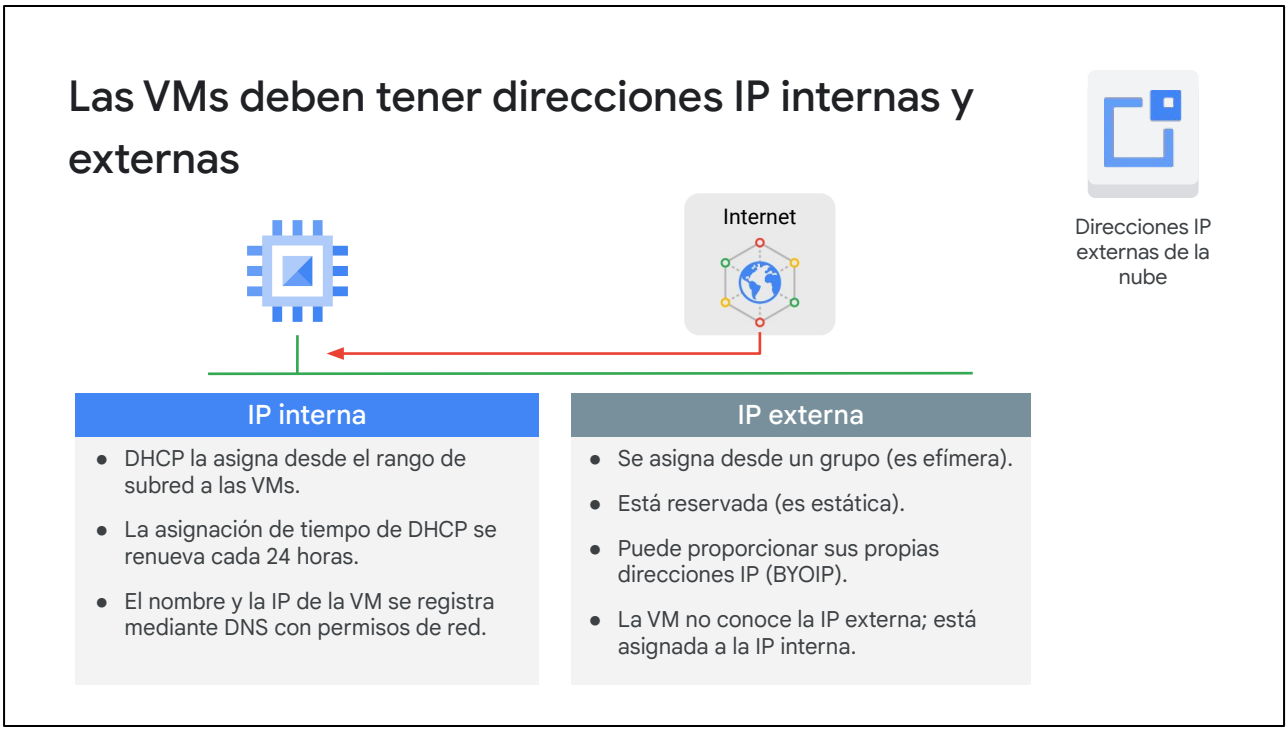
- No se puede superponer con otras subredes.
- El rango de IP debe ser un bloque CIDR válido.
- Los rangos de IP de las nuevas subredes deben estar dentro de rangos de IP válidos.
- Se puede expandir, pero no reducir.
- El modo automático se puede expandir de /20 a /16.
- Evite las subredes grandes.



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.



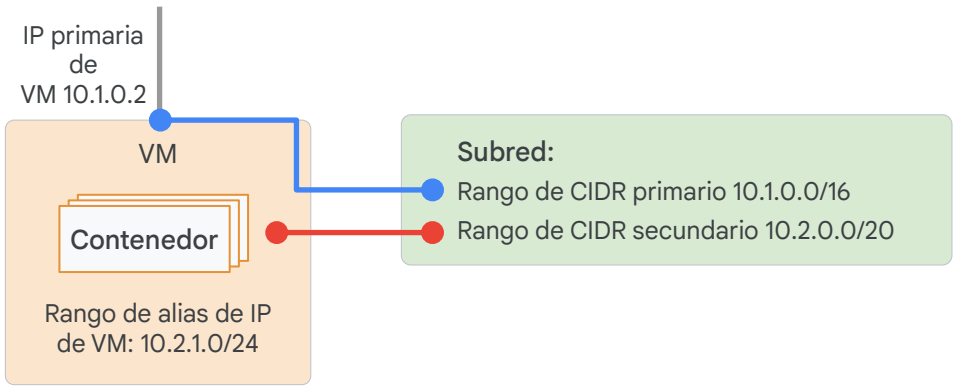
En Google Cloud, cada máquina virtual puede tener dos direcciones IP asignadas. Una de ellas es interna y se asigna internamente con DHCP. Todas las VMs que se inicien y todos los servicios que dependan de una máquina virtual recibirán una dirección IP interna. Algunos ejemplos de estos servicios son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

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/]

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.

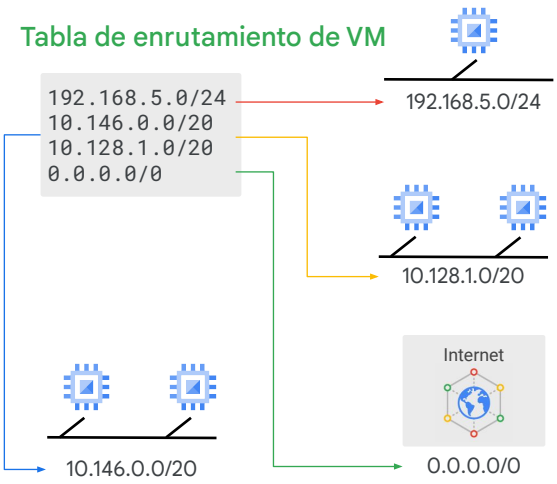
A pesar de que las rutas satisfacen la mayor parte de sus necesidades comunes de enrutamiento, también puede crear rutas especiales que anulen a las otras.

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 estáen notación CIDR.
- El tráfico solo se entrega si también coincide con una regla de firewall.

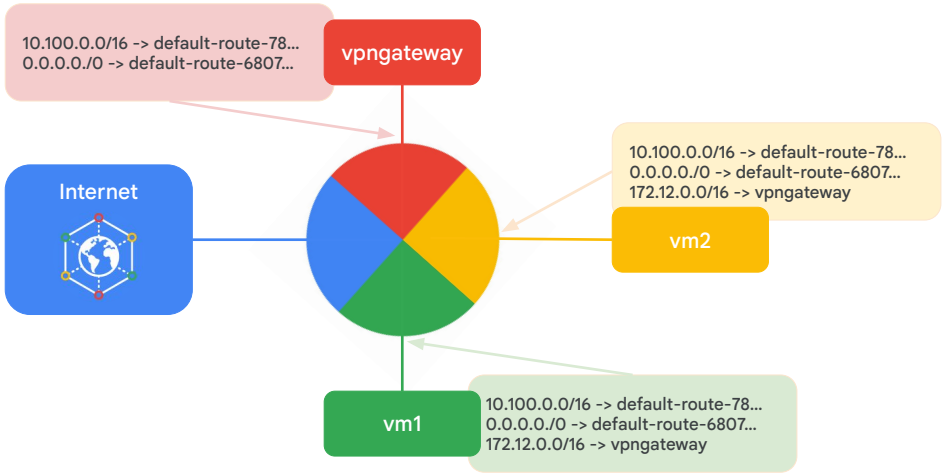


Las rutas hacen coincidir los paquetes según su dirección IP de destino. Sin embargo, no se permitirá el tráfico que no coincida con una regla de firewall específica.

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.

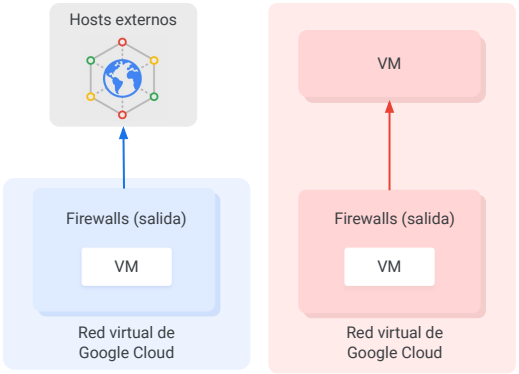
Las rutas asignan tráfico a redes de destino

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.

Caso de uso del firewall de Google Cloud: salida



Condiciones:

- Rangos CIDR de destino
- Protocolos
- Puertos

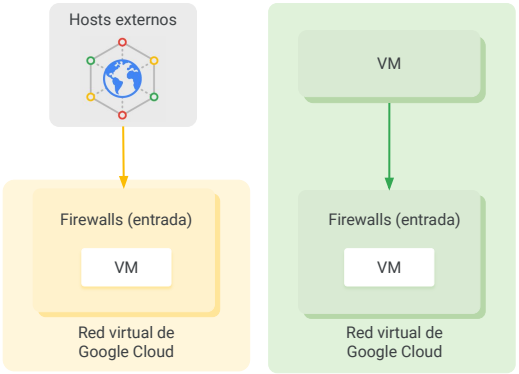
Acción:

- 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

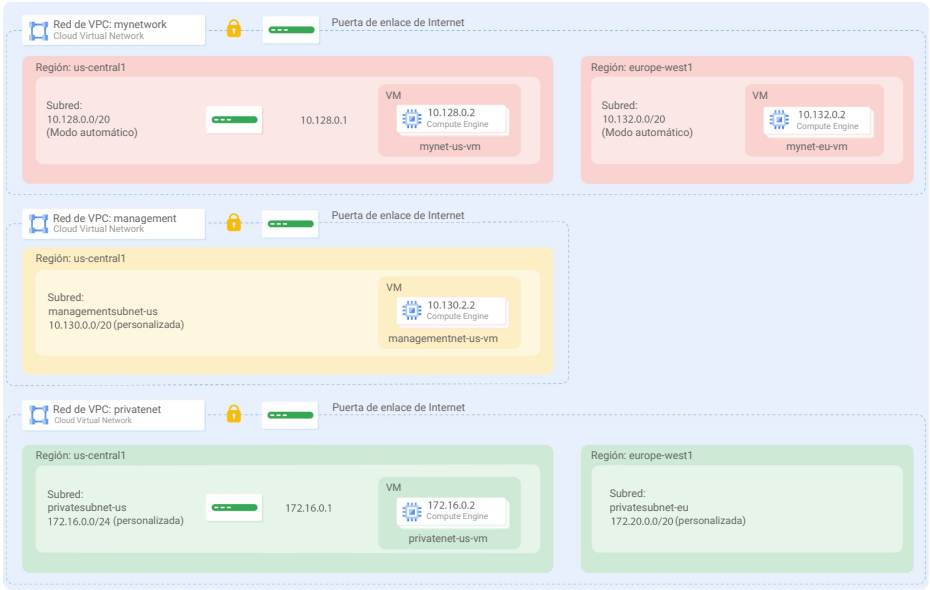
Acción:

- 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.

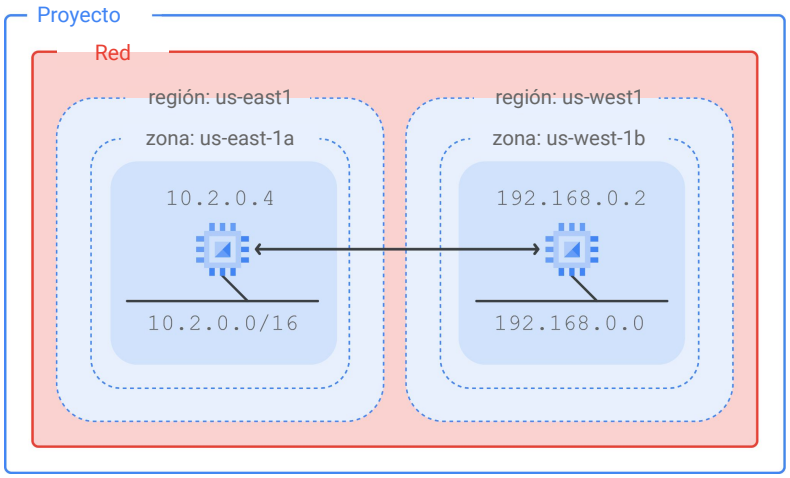
Los rangos de CIDR de origen pueden usarse para proteger una instancia de las conexiones no deseadas que provengan de redes externas o de rangos de IP de Google Cloud.

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.



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.

Globalización con varias regiones



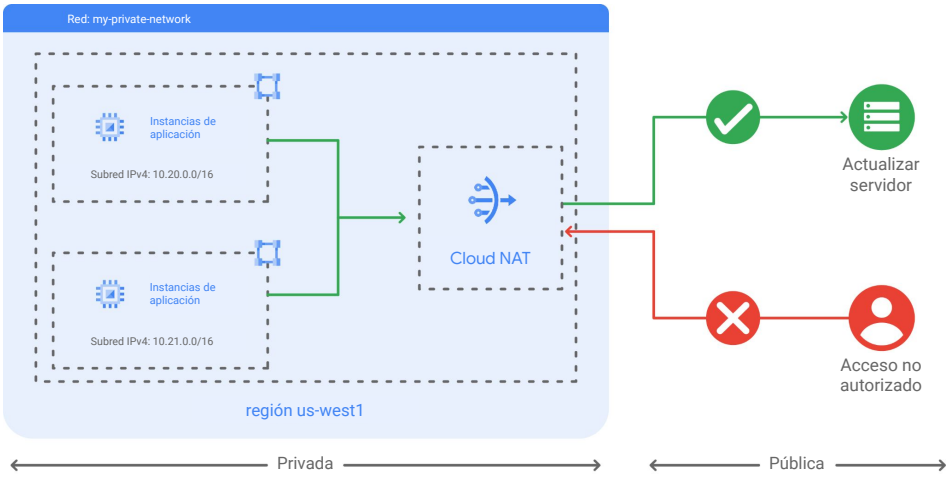
A continuación, analicemos la globalización.

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

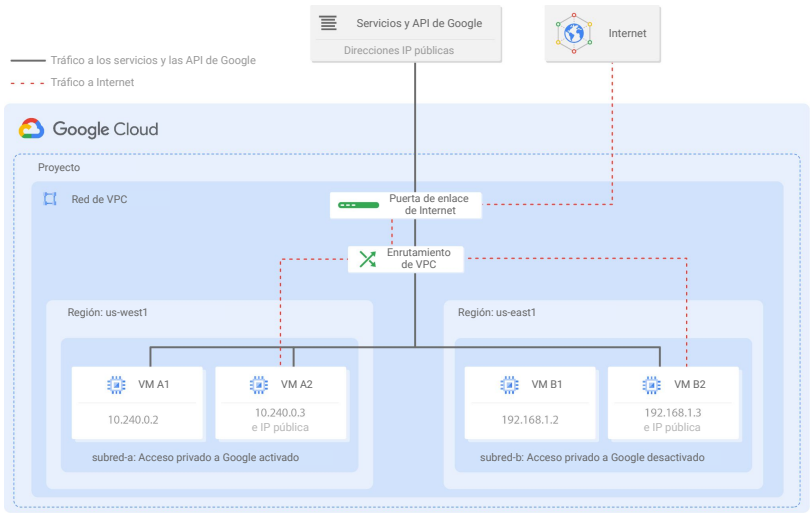


Como práctica recomendada de seguridad general, sugerimos que, cuando sea posible, use solo direcciones IP internas asignadas a sus instancias de VM.

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.