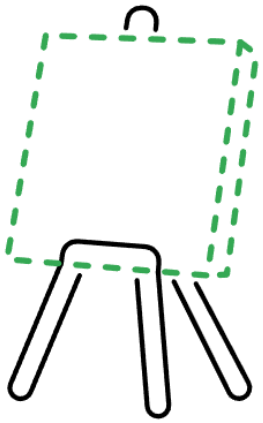
VPC Personalizada

Elaborada por: M. en C. Ukranio Coronilla

Creando una VPC Personalizada

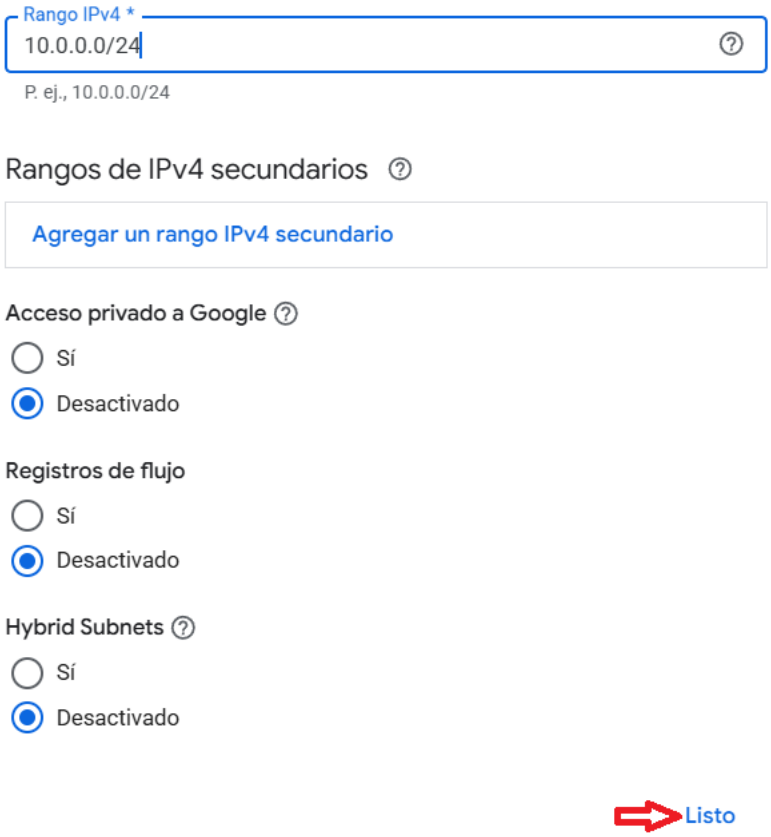
Vamos ahora a crear una red VPC personalizada, por lo que primero creamos un proyecto nuevo de nombre **VPC-personalizada** el cual tendrá una red default la cual tendremos que borrar, por lo que seleccionamos todas las reglas de firewall explicitas y damos click en BORRAR . Posteriormente damos click a la hamburguesa y seleccionamos: **Red de VPC -> Redes de VPC**. Damos click en la red predeterminada default y después en BORRAR LA RED DE VPC y esperamos a que se borre la red VPC para finalmente dar click en ACTUALIZAR y nos muestre que



No hay redes de VPC

Ahora para crear la red VPC, damos click en CREAR RED DE VPC , le asignamos como nombre **vpc-practica** y se selecciona el Modo de creación de subred como Personalizado para poder agregar manualmente cada subred. Para la Nueva subred le ponemos el nombre descriptivo **subred-us-central1** y

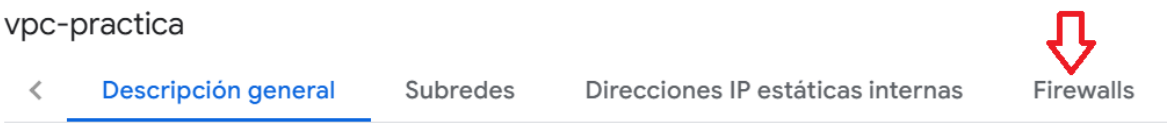
seleccionamos la región **us-central1**. El rango de IPv4 principal lo asignamos como **10.0.0.0/24**, dejamos las demás opciones sin modificar y damos click en la palabra **Listo** como como señala la flecha roja en la imagen:



En la sección Reglas de firewall podemos seleccionar reglas predefinidas similares a las reglas implícitas y explicitas vistas en la práctica anterior, pero en este caso crearemos posteriormente nuestras propias reglas por lo que damos click en CREAR para crear nuestra red sin reglas de firewall.

Configurar las Reglas de Firewall

Para configurar las reglas de firewall damos click a la hamburguesa y seleccionamos: **Red de VPC -> Redes de VPC** y damos click en la red que acabamos de crear vpc-practica. Posteriormente damos click en la pestaña Firewalls:



y posteriormente en el botón Agregar regla de firewall para agregar una regla de firewall sencilla que permita el tráfico entrante del protocolo ICMP hacia nuestra red desde cualquier lugar usando la siguiente configuración:

Nombre: **allow-icmp-ssh**

Prioridad: **60000**

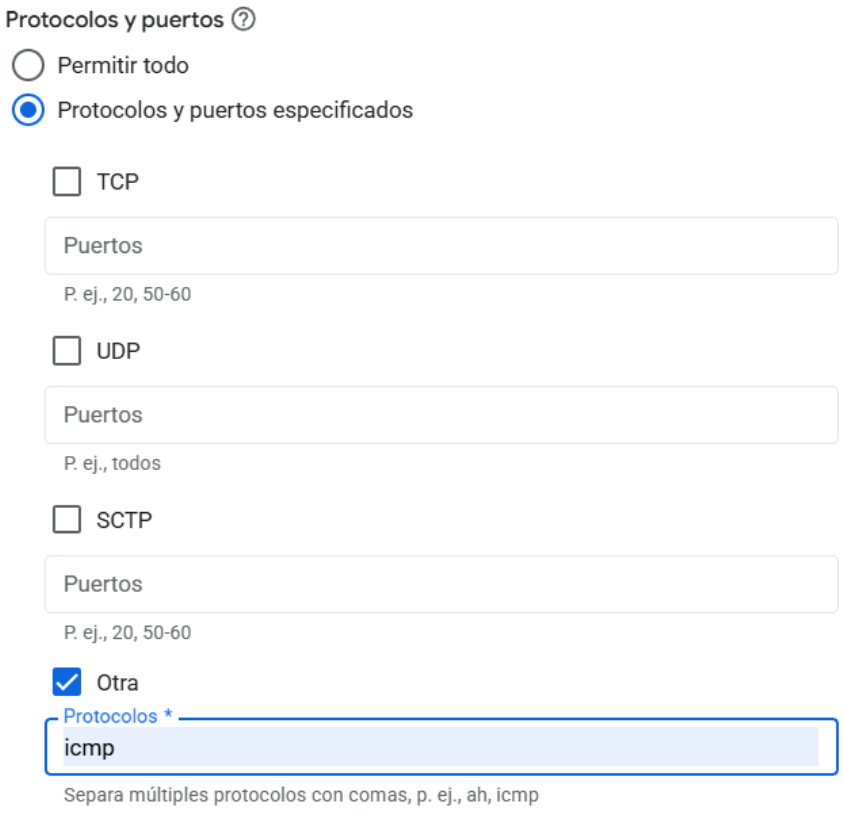
Dirección de tráfico: **Entrada**

Acción en caso de coincidencia: **Permitir**

Destinos: **Todas las instancias de la red**

Rangos de IPv4 de origen: **0.0.0.0/0**

Y por último en **Protocolos y puertos** seleccionamos el protocolo icmp:



Finalmente damos click en CREAR y esperamos a que se cree la regla de firewall.

Para probar que funciona nuestra red con el firewall especificado, creamos una máquina virtual en la subred **subred-us-central1**. Damos click a la hamburguesa ☰ y

seleccionamos: **Compute Engine -> Instancias de VM** y posteriormente en CREAR INSTANCIA.

Configuramos la instancia con los siguientes parámetros:

Nombre: **vm-subred-us-central1**

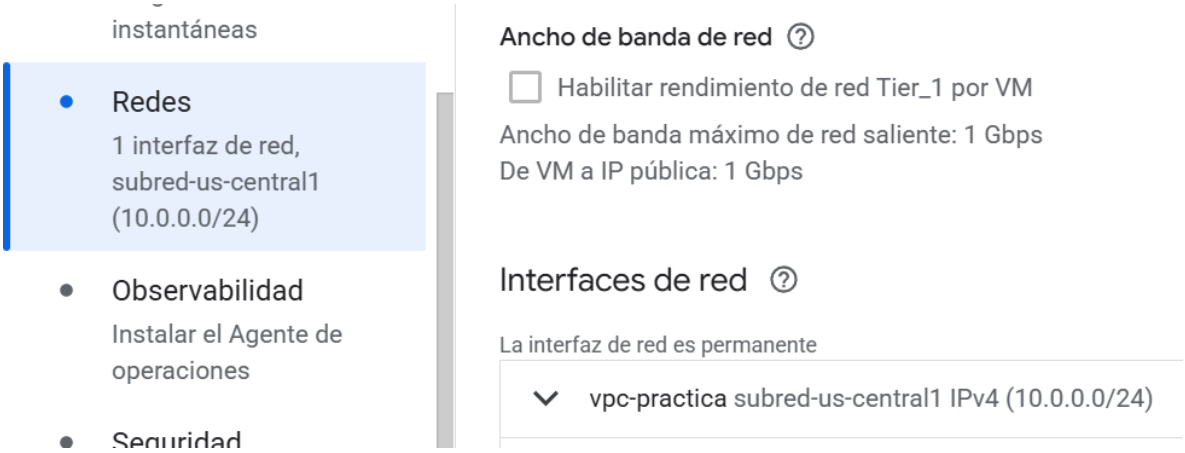
Región: **us-central1**

Zona: **Cualquiera**

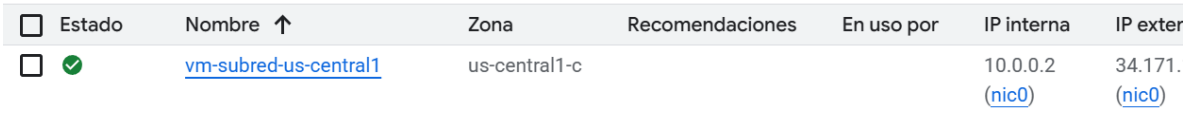
Series: **E2**

Tipo de máquina: e2-micro (2 CPU virtuales, 1 núcleos, 1 GB de memoria)

Si damos click en la sección de **Redes** podremos observar que se encuentra en la subred que acabamos de crear:



Finalmente le damos en CREAR y nos muestra la instancia creada con la IP interna dentro de nuestra subred:



Dado que el comando **ping** genera un mensaje que utiliza el protocolo ICMP, debería estar permitido hacerle ping a la IP externa desde nuestra computadora en casa hasta la máquina virtual que acabamos de crear (pruébelo).

Ahora cree otra máquina virtual idéntica llamada **vm2-subred-us-central1** en la misma subred e intente abrir una sesión SSH lo cual no será posible hasta que agregue la regla que nos faltó ¿Cuál fue? 🙁

Abierta la sesión SSH intente hacerle ping a la máquina **vm-subred-us-central1** usando la IP interna y la IP externa y observe en el promedio de tiempo que ocuparon los paquetes transmitidos con cuál de las dos IPs hay más latencia y con cual menos.

Regla para restringir el tráfico

Para restringir todo el tráfico ICMP cree una nueva regla de firewall llamada **deny-icmp** con las siguientes configuraciones:

Nombre: **deny-icmp**

Prioridad: Pruebe primero con 60001 y después edite la regla para cambiarla a 59999. Recuerde que a menor valor mayor prioridad.

Dirección de tráfico: **Entrada**

Acción en caso de coincidencia: **Rechazar**

Destinos: **Todas las instancias de la red**

Rangos de IPv4 de origen: **0.0.0.0/0**

Y por último seleccionamos el protocolo **icmp**:

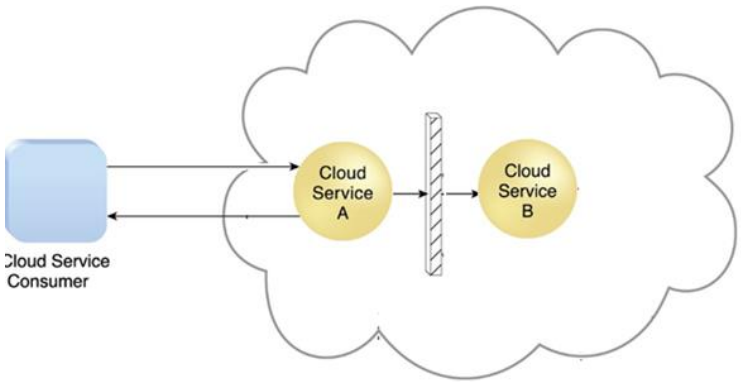
Verifica que, después de aplicar esta regla no podrás hacer uso de ping ni desde tu PC ni entre máquinas virtuales usando la IP externa o interna, pues solo el tráfico SSH sigue estando permitido, pero no el protocolo icmp.

En GCP no se cobra por crear una VPC o por implementar reglas de firewall, sin embargo, **si se cobra por el tráfico de salida de datos desde las instancias a**

Internet o entre regiones. El tráfico entre zonas dentro de la misma región es gratuito.

Ejercicio

De acuerdo con la siguiente figura, para mantener la seguridad en el servicio B (backend) se implementa un firewall para impedir el acceso a cualquier usuario consumidor de servicios en la nube, de tal manera que sólo la IP del servicio en la nube A (frontend) pueda acceder al servicio B.



En un nuevo proyecto de GCP cree una red VPC personalizada con las dos subredes (frontend y backend) en la misma región (de otro modo habría que agregar otra regla default-allow-internal como en la práctica anterior), con una instancia en cada subred de manera que se permita el tráfico HTTP desde internet al frontend, también se debe permitir el tráfico interno del frontend al backend mientras que por seguridad se debe bloquear el acceso externo al backend.

Envíe una captura de pantalla de la consola de Google mostrando las reglas que se incluyeron, así como una breve explicación de las mismas. También adjunte tres capturas de pantalla mostrando:

1. Al servidor HTTP cuyo código revisamos en clase ejecutándose en una sesión de SSH y en la instancia dentro de la subred de frontend en el puerto 80 mientras que es accedida con curl desde su LAP.
2. En una sesión SSH de la instancia en la subred frontend ejecutar curl hacia la IP interna de la instancia en la subred backend en la cual se ejecuta otro servidor HTTP en el puerto 8080, el cual también debería responder.
3. Desde la terminal en su LAP intente acceder con curl hacia la IP de la instancia en la subred backend donde no debería permitirse el acceso.