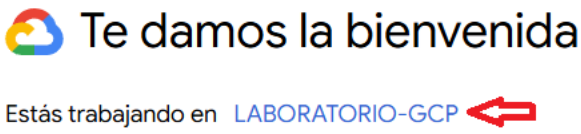
VPC y Reglas de Firewall

Elaborada por: M. en C. Ukranio Coronilla

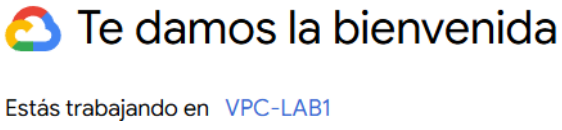
En GCP, VPC significa Virtual Private Cloud (Nube Privada Virtual), y se trata de una red privada virtual (versión virtual de una red física) que permite a recursos como las máquinas virtuales, bases de datos y otros servicios en la nube se comuniquen entre sí de manera segura.

Cada proyecto de GCP tiene una red denominada **default** con sus subredes, rutas y reglas de firewall. Para comprobarlo vamos a la consola de GCP y creamos un proyecto nuevo de nombre VPC-LAB1 dando click en (en mi caso estoy en un proyecto llamado LABORATORIO-GPC):



Y posteriormente en PROYECTO NUEVO donde introducimos el nombre del proyecto. Ahora elegimos ese nuevo proyecto dando click en

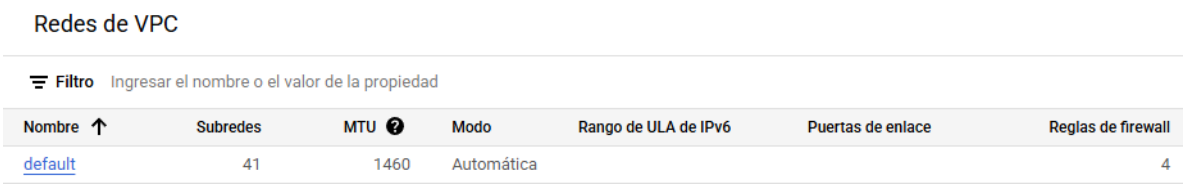
Y posteriormente damos click en el proyecto VPC-LAB1 que acabamos de crear con lo que aparece:



De aquí en adelante se recomienda crear un proyecto en cada práctica para evitar algún conflicto de configuración y al finalizar la práctica borrar el proyecto como se indica al final de esta práctica.

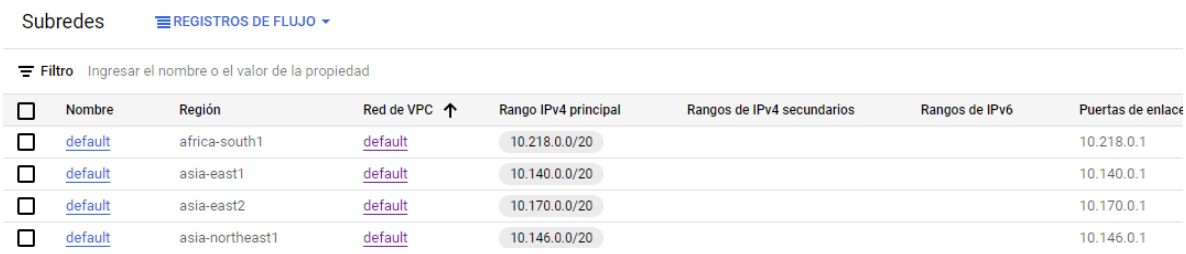
Subredes

Para visualizar las redes de VPC existentes le damos click a la hamburguesa ☰ en la esquina superior izquierda para ver el panel y seleccionamos **Red de VPC -> Redes de VPC** (es posible que te pida antes habilitar la Compute Engine API si no está habilitada). En este caso nos muestra una sola red de VPC de nombre **default** la cual contiene 41 subredes:



Las subredes pueden estar ubicadas en regiones distintas, pero al encontrarse dentro de la misma red VPC no requieren una VPN para comunicarse entre ellas. Las subredes permiten segmentar la red VPC y así utilizar una subred para "backend" y otra para "frontend", por ejemplo.

Para ver los detalles de las subredes damos click en SUBREDES DEL PROYECTO ACTUAL con lo que aparece la lista de subredes:



Observe que existen subredes en regiones distintas cuyas direcciones de IP son privadas y se utilizan para redes internas no enrutables en internet. En la columna **Rango IPv4 principal** se encuentran los rangos de IPs disponibles en cada subred. Si tomamos como ejemplo el primer renglón tenemos la red base: 10.218.0.0 y la máscara de subred /20 que nos permite inferir cuántas direcciones están disponibles en esa subred. En este caso **los primeros 20 bits** de la dirección IP están fijos para la red, y los **restantes 12 bits** pueden tener cualquier valor (porque una dirección IPv4 tiene 32 bits). Esto significa que pueden existir 2^{12} = 4096 direcciones IP en total, aunque hay que quitar las 5 direcciones que GCP usa para la puerta de enlace, DNS interno, etc. Para este caso tendríamos el siguiente rango de direcciones IP: 10.218.0.0 a 10.218.15.255 aunque este rango se usa para cargas grandes pues una máscara /24 es más común en producción.

Ejercicio 1

Tome un rango IPv4 de una de las subredes que aparecen en su lista y calcule el rango de IPs que le correspondería, escriba lo cálculos que hizo para obtener dicho rango.

Firewall

Para proteger nuestra red de GCP y/o controlar el tráfico entre las instancias y/o recursos de GCP se utiliza un conjunto de reglas que permitan o denieguen el tráfico de red conocidas como reglas de firewall.

Un ejemplo de reglas de firewall es permitir el acceso de paquetes que usan el protocolo HTTP/HTTPS al frontend, y bloquear el tráfico desde cualquier fuente externa al backend, aunque se permite el tráfico entre el frontend y el backend.

Cada regla de firewall se especifica mediante los siguientes parámetros principales:

Parámetro	Descripción
name	Nombre de la regla única dentro del proyecto. Se recomienda usar nombres entendibles en las reglas, por ejemplo con el formato: *ingress/egress-allow/deny-service-to/from-location*
direction	Especifica la dirección del tráfico, si es **ingress** se trata de tráfico entrante a la red, y si es **egress** se trata del saliente.
action	**allow** permite el tráfico que coincide con la regla, mientras que **deny** bloquea el tráfico que coincide con la regla.
priority	Es un valor numérico entre 0 y 65535 que indica el orden en que se evalúan las reglas. Una regla con prioridad 100 se evaluará antes o tiene mayor prioridad que una regla con prioridad 1000 (el cual es el valor default).
Rango de IPs	Rango que especifica el origen o destino del tráfico. Por ejemplo el rango origen 0.0.0.0/0 especifica que el tráfico puede venir desde cualquier IP.
Protocolos y puertos	Especifica los protocolos y puertos afectados por la regla en un formato **protocol:port**. Por ejemplo: **tcp:22**(SSH), **udp:53**(DNS). También se puede escribir: **icmp**(refiriéndose al ping) o **all**(refiriéndose a todos los protocolos).
Objetivos afectados por la regla	Determinan las instancias especificas dentro de la red a las que afecta la regla. **targetTags**: Etiquetas que identifican las instancias a las que se aplica la regla. **targetServiceAccounts**: Cuentas de servicio que identifican las instancias a las que se aplica la regla.

Reglas de firewall

Al crear un proyecto ya existen dos reglas de firewall implícitas en la VPC. La primera regla tiene dirección **egress** y especifica que una instancia puede enviar tráfico hacia cualquier destino, con la prioridad más baja 65535. La segunda regla tiene dirección **ingress** e impide las conexiones entrantes desde cualquier destino con la prioridad más baja. Adicionalmente tenemos otras cinco reglas explícitas que podemos visualizar al dar click en Firewall sobre el panel izquierdo (es necesario dar click en los iconos ⌄ para ver el contenido de cada fila como se muestra en la imagen):

Nombre	Tipo	Destinos	Filtros	Protocolos/puertos	Acción	Prioridad	Red ↑
default-allow-icmp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	icmp	Permitir	65534	default
default-allow-internal	Entrada	Aplicar a todas	Intervalos de IP: 10.128.0.0/9	tcp:0-65535 udp:0-65535 icmp	Permitir	65534	default
default-allow-rdp	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:3389	Permitir	65534	default
default-allow-ssh	Entrada	Aplicar a todas	Intervalos de IP: 0.0.0.0/0	tcp:22	Permitir	65534	default

Estas reglas nos indican que se permite el tráfico de entrada del protocolo de control ICMP, de escritorio remoto RDP y de canal seguro SSH proveniente desde cualquier IP (0.0.0.0/0) y con la prioridad más baja. También incluye la regla default-allow-internal que permite todo el tráfico ICMP, TCP y UDP dentro de la red VPC (10.128.0.0/9). Esta regla permite que si tengo dos instancias en subredes distintas puedan hacerse ping, conectarse por SSH, enviarse datos, etc.

Por seguridad se recomienda eliminar una o varias de estas reglas. Minimizar la exposición directa a Internet (evitar direcciones 0.0.0.0/0). Crear una regla de firewall que bloquee el tráfico saliente de todos los puertos y protocolos, anulando la regla implícita de envío hacia cualquier destino, y con una prioridad más alta permitir sólo los puertos necesarios. Para lograr esto se requiere de una red VPC personalizada.

Ejercicio 2

Dentro del proyecto VPC-LAB1 cree un par de instancias con máquinas f1-micro utilizando el Cloud Shell y el comando gcloud (cada instancia debe encontrarse en una subred distinta). Posteriormente use esas instancias y si es necesario su terminal de la LAP para mostrar que están activas cada una de las seis reglas de firewall que se acaban de describir (excepto la regla **default-allow-rdp** porque no

trabajaremos instancias windows). Explique lo que hizo para probar cada regla y agregue las capturas de pantalla que lo demuestran.

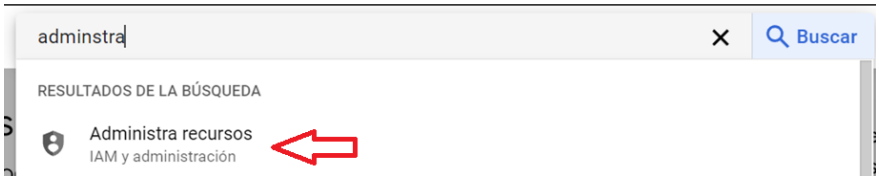
Borrar proyecto

En las prácticas es posible que se generen cargos al dejar sin querer algún recurso activo por lo que se recomienda **después de terminar cada práctica** borrar el proyecto actual y crear uno nuevo para cada práctica nueva.

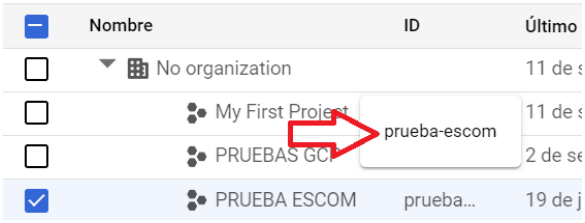
Primero buscamos la página de **Facturación**:

Después damos click en Administrar la cuenta de facturación y en el proyecto que queremos eliminar damos click en ⋮ y se selecciona Inhabilitar facturación.

Posteriormente buscamos la página **Administra Recursos**:



Se le da click en la casilla del proyecto que se desea borrar, se apunta el ID del proyecto porque es necesario introducirlo:



Posteriormente damos click en BORRAR y nos aparece una nueva ventana donde introducimos el ID y posteriormente damos click en APAGAR DE TODOS MODOS.