



Instituto Politécnico Nacional

ESCUELA SUPERIOR DE CÓMPUTO

CLASE 27 - VPC PERSONALIZADA

Sistemas Distribuidos
Ukranio Coronilla Contreras

Luciano Hernández Jonathan

7CM3

Abril 30, 2025

1 Reglas de firewall.

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?

Para que sea posible acceder desde el ssh es necesario crear la regla de firewall allow-ssh que permite la entrada del protocolo tcp en el puerto 22, el cual es desde donde se accede al ssh. Una vez configurado, ya funciona de manera correcta. La configuración de firewall es la que se muestra a continuación:

Nombre	Tipo	Destinos	Filtros	Protocolos/puertos	Acción	Prioridad	Red ↑	Registros
allow-icmp-ssh	Entrada	Aplicar a	Intervalos	icmp	Permitir	60000	vpc-practica	Desactiva
allow-ssh	Entrada	Aplicar a	Intervalos	tcp:22	Permitir	60000	vpc-practica	Desactiva

Figure 1: Allow-ssh

2 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.

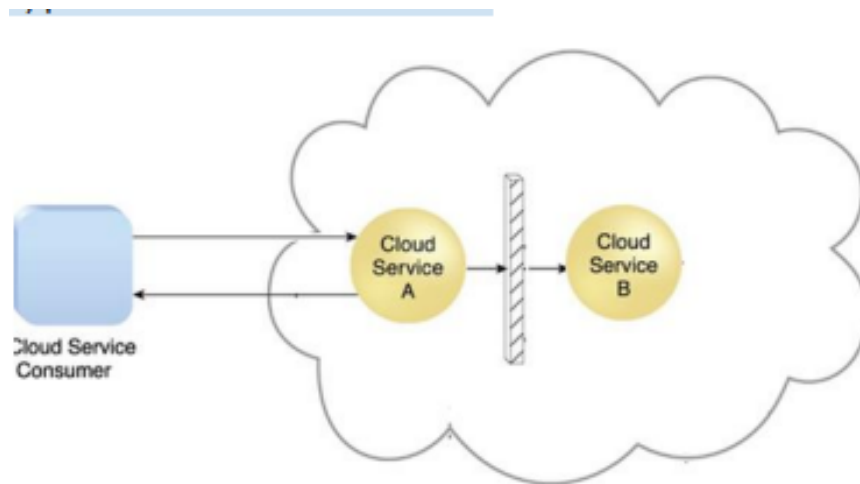


Figure 2: Caption

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 tres capturas de pantalla mostrando:

- 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.

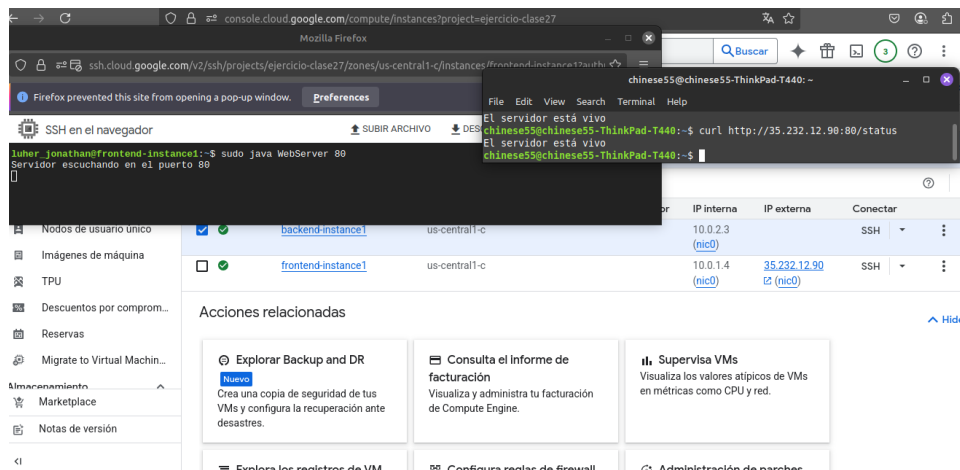


Figure 3: Prueba1

- 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.

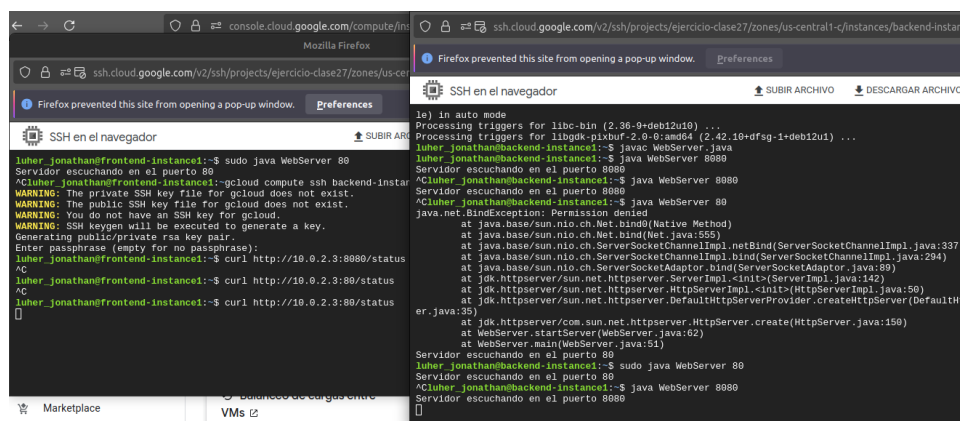


Figure 4: Caption

Tuve un error en alguna configuración del backend por lo que no pude resolver de manera correcta esta prueba, pues el frontend debió ser capaz de conectarse con la ip interna que posee, pues como se ve, no tiene ip externa.

- 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

The screenshot shows the Google Cloud Platform console for VM instances. A table lists two instances in the 'us-central1-c' zone. The first instance has an internal IP of 10.0.2.3 and an external IP of 35.232.12.90. The second instance has an internal IP of 10.0.1.4 and an external IP of 35.232.12.90. A terminal window is open, showing the command 'curl http://35.232.12.90/status' and the output 'El servidor está vivo'.

	Zona	Recomendaciones	En uso por	IP interna	IP externa	Conectar
1	us-central1-c			10.0.2.3 (nic0)	35.232.12.90 (nic0)	SSH
1	us-central1-c			10.0.1.4 (nic0)	35.232.12.90 (nic0)	SSH

```
chinese55@chinese55-ThinkPad-T440: ~  
File Edit View Search Terminal Help  
chinese55@chinese55-ThinkPad-T440:~$ curl http://35.232.12.90/status  
El servidor está vivo  
chinese55@chinese55-ThinkPad-T440:~$ curl http://10.0.2.3/status
```

Figure 5: Caption