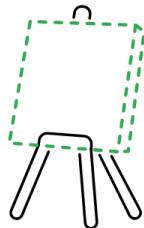


Clase 27

Red por defecto eliminada

<input type="checkbox"/>	Nombre ↑	Subredes	MTU ⓘ	Modo	Rango de ULA de IPv6	Puertas de enlace	Parámetros de configuración del registro de flujos ⓘ
--------------------------	----------	----------	-------	------	----------------------	-------------------	--



No hay redes de VPC

Una red de nube privada virtual (VPC) es una versión virtual de una red física, implementada dentro de la red de producción de Google. [Más información ⓘ](#)

Creando la VPC

← Crear una red de VPC

Nombre *

vpc-practica



Se permiten letras minúsculas, números y guiones

Descripción

Unidad de transmisión máxima (MTU) —

1460



Configurar el perfil de red ⓘ

Modo de creación de subred ⓘ

Personalizado

Automático

Creando la Subred

^ Nueva subred

Nombre * ?

Se permiten letras minúsculas, números y guiones

Descripción

Región * ?

Tipo de pila de IP ?

IPv4 (una sola pila)

IPv4 e IPv6 (pila doble)

IPv6 (pila única)

Rango IPv4 principal

Asociar con un rango interno
Usa un rango interno para especificar el rango de direcciones IP internas de la subred. La subred se puede asociar con un rango interno completo o solo con una parte del rango.

Rango IPv4 * ?

P. ej., 10.0.0.0/24

Acceso privado a Google ?

Sí

Desactivado

Registros de flujo

Sí

Desactivado

Hybrid Subnets ?

Sí

Desactivado

[Listo](#)

Redes de VPC		Administrar registros de flujo		
Filtro		Escribir el nombre o valor de la propiedad		
Nombre	↑	Subredes	MTU ?	Modo
<input type="checkbox"/> vpc-practica		1	1460	Personalizado

Configurar las reglas de Firewall

No encontré el botón indicado en documento, pero hice clic en el botón de crear regla de firewall de VPC:

vpc-practica

< Descripción general Subredes Direcciones IP estáticas internas Firewalls

Ver políticas Vista de reglas de firewall

Políticas jerárquicas

Filtro Escribir el nombre o valor de la propiedad

Nombre	↑ Orden de aplicación	Permiso de la implementación	Reglas de fi
No hay filas para mostrar			

Reglas de firewall de VPC **+ Crear regla de firewall de VPC** Actualizar

Filtro Escribir el nombre o valor de la propiedad

Nombre	Orden de aplicación	Permiso de la implementación	↑ Prioridad	De
No hay filas para mostrar				

Detalles de la regla de firewall

allow-icmp-ssh

Registros [?](#)
Desactivado
[Ver en el Explorador de registros](#)

Red
vpc-practica

Prioridad
60000

Dirección
Entrada

Acción en caso de coincidencia
Permitir

Etiquetas

-

Filtros de fuente

Rangos de IP	0.0.0.0/24
--------------	------------

Protocolos y puertos
icmp

Creando la VM

Configuración de la máquina

Nombre * (?)

Región * (?) Zona * (?)

La región es permanente

Google elegirá una zona en tu nombre, lo que maximizará la disponibilidad de las VMs. La zona es permanente.

De uso general Optimizado para procesamiento Con optimización de memoria
 Optimizada para almacenamiento GPU

Tipos de máquinas para cargas de trabajo comunes, optimizados en función del costo y la flexibilidad

Series (?)	Descripción	vCPUs (?)	Memory (?)	Plataforma
<input type="radio"/> C4	Rendimiento alto y constante	2 - 288	4 - 2,232 GB	Intel Emer
<input type="radio"/> C4A	Alto rendimiento coherente basado en ARM	1 - 72	2 - 576 GB	Google Ax
<input type="radio"/> C4D	Rendimiento alto y constante	2 - 384	3 - 3,072 GB	AMD Turin
<input type="radio"/> N4	Flexible y con optimización de costos	2 - 80	4 - 640 GB	Intel Emer
<input type="radio"/> C3	Rendimiento alto y coherente	4 - 192	8 - 1,536 GB	Intel Sapp
<input type="radio"/> C3D	Rendimiento alto y constante	4 - 360	8 - 2,880 GB	AMD Gen
<input checked="" type="radio"/> E2	Procesamiento diario de bajo costo	0.25 - 32	1 - 128 GB	Intel Broad
<input type="radio"/> M2	Procesamiento de memoria	0.25 - 32	0 - 64 GB	Intel Broad

Tipo de máquina

Elige un tipo de máquina con cantidades predeterminadas de CPU virtuales y memoria que se adapten a la mayoría de las cargas de trabajo. También puedes crear una máquina personalizada según las necesidades particulares de tu carga de trabajo. [Más información](#)

Configuración predeterminada Personalizado

e2-micro (2 CPU virtuales, 1 núcleo, 1 GB de memoria) (?)



vCPU

De 0.25 a 2 CPU virtuales (1 núcleo compartido)

Memory

1 GB

- **Protección de datos**
Programaciones de instantáneas
- **Redes**
1 interfaz de red, subred us-central1 (10.0.0.0/24)
- **Observabilidad**
Instalar el Agente de operaciones

Ancho de banda de red (?)

 Habilitar rendimiento de red Tier_1 por VM

Ancho de banda máximo de red saliente: 1 Gbps

De VM a IP pública: 1 Gbps

Interfaces de red (?)

La interfaz de red es permanente

nic0 vpc-practica subred-us-central1 IPv4 (10.0.0.0/24) (?) (trash)

Instancias de VM

Filtro Escribir el nombre o valor de la propiedad

<input type="checkbox"/>	Estado	Nombre ↑	Zona	Recomendaciones	En uso por	IP interna	IP externa	Conectar
<input checked="" type="checkbox"/>	vm-subred-us-central1		us-central1-c			10.0.0.2 (nic0)	136.116.0.123 (nic0)	SSH ⋮

Ejercicio

Reglas:

```
contla_mota_luisandres@cloudshell:~ (psyched-myth-477205-i5)$ gcloud compute firewall-rules list \
--filter="network='vpc-ejercicio' AND name~'(allow-ssh-all|allow-http-to-frontend|allow-internal-frontend-to-backend)'" \
--format="table(name,allowed,sourceRanges.list():label=SRC_RANGES,sourceTags.list():label=SRC_TAGS,targetTags.list():label=TARGET_TAGS
,priority)"
NAME: allow-ssh-all
ALLOWED: []
SRC_RANGES: 0.0.0.0/0
SRC_TAGS:
TARGET_TAGS: frontend,backend
PRIORITY: 1000

NAME: allow-http-to-frontend
ALLOWED: [{"IPProtocol": "tcp", "ports": ["80"]}]
SRC_RANGES:
SRC_TAGS: frontend
TARGET_TAGS: backend
PRIORITY: 1000

NAME: allow-internal-frontend-to-backend
ALLOWED: [{"IPProtocol": "tcp", "ports": ["8080"]}]
SRC_RANGES:
SRC_TAGS: frontend
TARGET_TAGS: backend
PRIORITY: 1000
```

allow-ssh-all: Regla de administración básica que habilita el acceso SSH (puerto 22) a vm-frontend y vm-backend desde cualquier origen. Se usa para conectarnos, configurar las máquinas, levantar servicios y ejecutar pruebas.

allow-http-to-frontend: Autoriza el tráfico HTTP (puerto 80) desde Internet únicamente hacia las instancias con la etiqueta frontend-server. Con esto el servicio público queda expuesto solo en el frontend y el backend permanece no accesible de forma directa.

allow-internal-frontend-to-backend: Regla clave de seguridad: permite que solo las instancias etiquetadas como frontend-server se comuniquen con las etiquetadas backend-server por el puerto 8080. Al usar etiquetas de origen y destino, se bloquea cualquier intento que no provenga del frontend, incluyendo accesos directos desde Internet.

Captura 1

```
C:\Users\luisc>curl.exe -i "http://34.10.36.150/status"
HTTP/1.1 200 OK
Server: nginx/1.22.1
Date: Tue, 04 Nov 2025 06:37:10 GMT
Content-Length: 23
Connection: keep-alive
```

El servidor está vivo

Captura 2

```
contla_mota_luisandres@cloudshell:~ (psyched-myth-477205-i5)$ BACKEND_INT=$(gcloud compute instances describe vm-backend --zone=us-central1-a --format='get(networkInterfaces[0].networkIP)')
contla_mota_luisandres@cloudshell:~ (psyched-myth-477205-i5)$ echo "BACKEND_INT=$BACKEND_INT"
BACKEND_INT=10.10.2.2
contla_mota_luisandres@cloudshell:~ (psyched-myth-477205-i5)$ gcloud compute ssh vm-frontend --zone=us-central1-a --command="curl -i http://$BACKEND_INT:8080/status"
% Total    % Received % Xferd  Average Speed   Time   Time     Time  Current
          Dload  Upload   Total Spent    Left  Speed
100    23  100    23    0      0  5708      0 --:--:-- --:--:--  7666
HTTP/1.1 200 OK
Date: Tue, 04 Nov 2025 06:41:40 GMT
Content-length: 23
El servidor está vivo
```

Captura 3

```
C:\Users\luisc>curl -i --max-time 5 "http://34.60.116.198:8080/status" || echo "bloqueado/timeout (OK)"
curl: (28) Connection timed out after 5002 milliseconds
"bloqueado/timeout (OK)"

C:\Users\luisc>
```