



en centros de datos, todas conectadas mediante una red de área extensa (WAN) global. Las redes de VPC están aisladas de forma lógica unas de otras dentro de Google Cloud.

### Tarea 1. Explore la red predeterminada.

1. Ingrese a su cuenta de Google Cloud Platform
2. Cree un proyecto y selecciónelo (establézcalo como predeterminado)
3. En Cloud Console, en **Menú de navegación** () , haga clic en **Red de VPC > Redes de VPC**.

Observe la red **predeterminada** con sus subredes.

Cada subred está asociada con una región de Google Cloud y un bloque privado de CIDR conforme a RFC 1918 para su **rango de direcciones IP** internas y una **puerta de enlace**.

**Visualice las rutas.** Estas informan a las instancias de VM y la red de VPC cómo enviar tráfico desde una instancia a un destino, dentro de la red o fuera de Google Cloud. Cada red de VPC incluye algunas rutas predeterminadas para enrutar el tráfico entre sus subredes y enviar tráfico desde instancias aptas a Internet.

Para ello, haga clic en **Rutas**.

Observe que hay una ruta para cada subred y una para la **puerta de enlace de Internet predeterminada (0.0.0.0/0)**.

Estas rutas se administran por usted, pero puede crear rutas estáticas personalizadas para dirigir algunos paquetes a destinos específicos. Por ejemplo, puede crear una ruta que envíe todo el tráfico saliente a una instancia configurada como una puerta de enlace NAT.

**Visualice las reglas firewall.** Cada red de VPC implementa un firewall virtual distribuido que puede configurar. Con las reglas de firewall, puede controlar qué paquetes tienen permitido trasladarse a qué destinos. Cada red de VPC tiene dos reglas de firewall implícitas que bloquean todas las conexiones entrantes y permiten todas las conexiones salientes.

En el panel izquierdo, haga clic en Firewall.

Observe que hay 4 reglas de firewall de entrada para la red predeterminada:

- default-allow-icmp
- default-allow-rdp
- default-allow-ssh
- default-allow-internal

**Nota:** Estas reglas de firewall permiten el tráfico de entrada ICMP, RDP y SSH desde cualquier parte (0.0.0.0/0), y todo el tráfico TCP, ICMP y UDP dentro de la red (10.128.0.0/9). En las columnas Destinos, Filtros, Protocolos/puertos y Acción se explican estas reglas.

## Borre las reglas firewall

1. En el panel izquierdo, haga clic en **Firewall**.
2. Seleccione todas las reglas de firewall de red predeterminadas.
3. Haga clic en **Borrar**.
4. Haga clic en **Borrar** para confirmar la eliminación de las reglas de firewall.

VPC network Firewall CREATE FIREWALL RULE REFRESH CONFIGURE LOGS DELETE

You don't have required permissions: compute.organizations.setSecurityPolicy to view the firewall policies inherited by this project.

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#).

Filter Enter property name or value

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last hit	Insights
<input checked="" type="checkbox"/> default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0	icmp	Allow	65534	default	Off	—	—	▼
<input checked="" type="checkbox"/> default-allow-internal	Ingress	Apply to all	IP ranges: 10.12	tcp:0-65535 udp:0-65535 icmp	Allow	65534	default	Off	—	—	▼
<input checked="" type="checkbox"/> default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0	tcp:3389	Allow	65534	default	Off	—	—	▼
<input checked="" type="checkbox"/> default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0	tcp:22	Allow	65534	default	Off	—	—	▼

## Borre la red predeterminada

1. En el panel izquierdo, haga clic en **Redes de VPC**.
2. Seleccione la red **predeterminada**.
3. Haga clic en **Borrar la red de VPC**.
4. Haga clic en **Borrar** para confirmar la eliminación de la red **predeterminada**. Espere a que se borre la red antes de continuar.
5. En el panel izquierdo, haga clic en **Rutas**. Observe que no hay rutas.
6. En el panel izquierdo, haga clic en **Firewall**. Observe que no hay reglas de firewall.


**Nota:** Sin una red de VPC, no hay rutas ni reglas de firewall.

## Intente crear una instancia de VM

1. En el **menú de navegación** (≡), haga clic en **Compute Engine > Instancias de VM**.
2. Haga clic en **Crear instancia**.
3. Acepte los valores predeterminados y haga clic en **Crear**. Observe el error.
4. Haga clic en **Administración, seguridad, discos, redes, usuario único**.
5. Haga clic en **Herramientas de redes**. Observe el error **No hay ninguna red local disponible** en **Interfaces de red**.
6. Haga clic en **Cancelar**.


**Nota:** Como se esperaba, no puede crear una instancia de VM sin una red de VPC.

**Tarea 2: Cree una red de VPC e instancias de VM.** En esta tarea se creará una red en modo automático, con reglas de firewall y se conectarán dos instancias de VM.

1. En **Menú de navegación** () , haga clic en **Red de VPC > Redes de VPC**.
2. Haga clic en **Crear red de VPC**.
3. En **Nombre**, escriba **mynetwork**.
4. En **Modo de creación de subred**, haga clic en **Automático**.  
Las redes de modo automático crean subredes en cada región automáticamente.
5. En **Firewall**, seleccione todas las reglas disponibles. Son las mismas reglas de firewall estándar que tenía la red predeterminada. También se muestran las reglas **deny-all-ingress** y **allow-all-egress**, pero no puede marcarlas ni desmarcarlas porque están implícitas. Esas dos reglas tienen una **prioridad** más baja (los números enteros más altos indican prioridades más bajas), de modo que se consideren primero las reglas internas y de SSH, ICMP y RDP.
6. Haga clic en **Crear**. Cuando esté lista la red nueva, observe que se creó una subred para cada región.
7. Explore el rango de direcciones IP de las subredes en **us-central1** y **us-west1**.  
Se hará referencia a esto en los pasos siguientes.

**Nota:** Si alguna vez borra la red predeterminada, puede volver a crearla rápidamente. Para ello, deberá crear una red de modo automático como se describió anteriormente.


### **Crea una instancia de VM en us-central1**

1. En el **menú de navegación** () , haga clic en **Compute Engine > Instancias de VM**.
2. Haga clic en **Crear instancia**.
3. Especifique lo siguiente y deje los parámetros de configuración restantes con sus valores predeterminados:

Propiedad	Valor (escriba el valor o seleccione la opción como se especifica)
Nombre	mynet-us-vm-1
Región	us-central1
Zona	us-central1-a
Serie	E2
Tipo de máquina	e2-micro (2 CPU virtual, 1 GB de memoria)

4. Haga clic en **Crear**.

### **Crea una instancia de VM en us-west1**

1. En el **menú de navegación** () , haga clic en **Compute Engine > Instancias de VM**.
2. Haga clic en **Crear instancia**.
3. Especifique lo siguiente y deje los parámetros de configuración restantes con sus valores predeterminados:

Propiedad	Valor (escriba el valor o seleccione la opción como se especifica)
Nombre	mynet-us-vm-2
Región	us-west1
Zona	us-west1-a
Serie	E2
Tipo de máquina	e2-micro (2 CPU virtual, 1 GB de memoria)


4. Haga clic en **Crear**.

**Nota:** Las direcciones IP externas de ambas instancias de VM son efímeras. Si se detiene una instancia, las direcciones IP externas efímeras asignadas a la instancia se devuelven al grupo general de Compute Engine y quedan disponibles para que las usen otros proyectos. Cuando se vuelve a iniciar una instancia detenida, se le asigna una nueva dirección IP externa efímera. De manera alternativa, puede reservar una dirección IP externa estática, que asigna la dirección a su proyecto de forma indefinida hasta que la libere de manera explícita.

**Tarea 3: Explore la conectividad de las instancias de VM.** Se explorará la conectividad de las instancias de VM. Específicamente, tratará de acceder con SSH a sus instancias de VM mediante tcp:22 y hará ping a las direcciones IP internas y externas de sus instancias de VM con ICMP. Luego, explorará los efectos de las reglas de firewall en la conectividad. Para ello, eliminará las reglas individualmente.

### **Verifique la conectividad de las instancias de vm**

Las reglas de firewall que creó con **mynetwork** permiten el tráfico de entrada ICMP y SSH desde dentro de **mynetwork** (IP interna) y fuera de esa red (IP externa).

1. En Menú de navegación () , haga clic en **Compute Engine > Instancias de VM**. Observe las direcciones IP internas y externas de **mynet-us-vm-1**.
2. En **mynet-us-vm-1**, haga clic en **SSH** a fin de iniciar una terminal y conectarse.

**Nota:** Puede establecer una conexión SSH debido a la regla de firewall **allow-ssh**, que permite el tráfico entrante desde cualquier parte (0.0.0.0/0) para **tcp:22**. La conexión SSH funciona a la perfección porque Compute Engine genera una clave SSH para usted y la almacena en una de las siguientes ubicaciones:

3. Para probar la conectividad con la IP interna de **mynet-us-vm-1**, ejecute el siguiente comando, en el que deberá ingresar la IP interna de **mynet-us-vm-2**:  
`ping -c 3 <Ingrese aquí la IP interna de mynet-us-vm-2>`


Puede hacer ping a la IP interna de **mynet-eu-vm** debido a la regla de firewall **allow-internal**.

4. Para probar la conectividad con la IP externa de **mynet-us-vm-1**, ejecute el siguiente comando, en el cual deberá ingresar la IP externa de **mynet-us-vm-2**:  
`ping -c 3 <Ingrese aquí la IP externa de mynet-us-vm-2>`

**Nota:** Puede acceder con SSH a **mynet-us-vm-1** y hacer ping a las direcciones IP internas y externas de **mynet-us-vm-2** como se esperaba. Otra alternativa es acceder con SSH a **mynet-us-vm-2** y hacer ping a las direcciones IP internas y externas de **mynet-us-vm-1**, lo cual también funciona.

### Quite las reglas de firewall **allow-icmp**

Quite la regla de firewall **allow-icmp** y, luego, intente hacer ping a las direcciones IP interna y externa de **mynet-us-vm-2**.

1. En el **menú de navegación** () , haga clic en **Red de VPC > Firewall**.
2. Seleccione la regla **mynetwork-allow-icmp**.
3. Haga clic en **Borrar**.
4. Haga clic en **Borrar** para confirmar esta acción. Espere hasta que se borre la regla de firewall.
5. Regrese a la terminal SSH de **mynet-us-vm-1**.
6. Para probar la conectividad con la IP interna de **mynet-us-vm-2**, ejecute el siguiente comando, en el que deberá ingresar la IP interna de **mynet-us-vm-2**:  
`ping -c 3 <Ingrese aquí la IP interna de mynet-us-vm-2>`


Puede hacer ping a la IP interna de **mynet-us-vm-2** debido a la regla de firewall **allow-custom**.

7. Para probar la conectividad con la IP externa de **mynet-us-vm-2**, ejecute el siguiente comando, en el cual deberá ingresar la IP externa de **mynet-us-vm-2**:  
`ping -c 3 <Ingrese aquí la IP externa de mynet-eu-vm>`

**Nota:** El 100% de pérdida de paquetes indica que no puede hacer ping a la IP externa de **mynet-us-vm-2**. Esto es normal porque borró la regla de firewall **allow-icmp**.

### Quite las reglas de firewall allow-custom

Quite la regla de firewall **allow-custom** y, luego, intente hacer ping a la dirección IP interna de **mynet-us-vm-2**.


1. En el **menú de navegación** () , haga clic en **Red de VPC > Firewall**.
2. Seleccione la regla **mynetwork-allow-custom**.
3. Haga clic en **Borrar**.
4. Haga clic en **Borrar** para confirmar esta acción. Espere hasta que se borre la regla de firewall.
5. Regrese a la terminal SSH de **mynet-us-vm-1**.
6. Para probar la conectividad con la IP interna de **mynet-us-vm-2**, ejecute el siguiente comando, en el que deberá ingresar la IP interna de **mynet-us-vm-2**:  
`ping -c 3 <Ingrese aquí la IP interna de mynet-us-vm-2>`

**Nota:** El **100% de pérdida de paquetes** indica que no puede hacer ping a la IP interna de **mynet-us-vm-2**. Esto es normal porque borró la regla de firewall **allow-custom**.

7. Cierre la terminal **SSH** con el comando `exit`

### Quite las reglas de firewall allow-ssh

Quite la regla de firewall **allow-ssh** y, luego, intente acceder con SSH a **mynet-us-vm-1**.

1. En el **menú de navegación** () , haga clic en **Red de VPC > Firewall**.
2. Seleccione la regla **mynetwork-allow-ssh**.
3. Haga clic en **Borrar**.
4. Haga clic en **Borrar** para confirmar esta acción.
5. Espere hasta que se borre la regla de firewall.
6. En el **menú de navegación**, haga clic en **Compute Engine > Instancias de VM**.
7. En **mynet-us-vm-1**, haga clic en **SSH** a fin de iniciar una terminal y conectarse.

**Nota:** El mensaje **Error de conexión** indica que no se puede establecer la conexión SSH a **mynet-us-vm-1** porque se borró la regla de firewall **allow-ssh**.

**¡ Felicitaciones ¡**

**RECOMENDACIONES /  
OBSERVACIONES**

Ninguna