**Virtual Private Cloud**

Es una forma de establecer conectividad entre los recursos que tengamos en la nube.

Ambiente de red virtual, **aislado** y **privado** que se basa en el concepto de red definida por software.

Existe una red global privada (tiene alcance global). Es decir nos permite conectar todos nuestros recursos a la VPC sin importar la región en que estén.

**Subredes**

Las VPC se forman de subredes. Una VPC debe tener al menos una subred.

Las subredes tienen alcance regional. Es decir, podemos conectar recursos que están en diferentes zonas de una región usando la subred.

Las subredes tienen asociados rangos de IPs, se usan para asignar IPs privadas a los recursos que están asociados a la subred.

**Tipos de VPC**

* **Default**: Crea una subred en todas las regiones de GCP, crea algunos Firewalls
* **Auto Mode**: Similar a la anterior, pero es expandible a /16.
* **Custom Mode**: No crea las subredes por defecto, se tiene control total de las IPs. Expandible a cualquier tamaño RFC 1918

## Rangos de subred

Cuando se crea una subred, se debe definir su rango principal de direcciones IP.

Las principales direcciones internas para los recursos (instancias de VM, balanceadores de carga internos y reenvío de protocolo interno) son del rango principal de la subred.

#### Limitaciones

* El rango de IP principal de la subred se puede expandir, pero no reemplazar ni reducir, después de que se haya creado la subred.
* Se puede eliminar y reemplazar el rango de direcciones IP secundarias de una subred solo si ninguna instancia está usando ese rango.
* El tamaño mínimo del rango primario o secundario es de ocho direcciones IP. Lo que significa que, la máscara de subred más larga que puede usar es / 29.
* Los rangos validos los pueden encontrar en <https://cloud.google.com/vpc/docs/vpc#valid-ranges>

VPC default no se recomienda en producción porque tenemos menos control cuando se genera el rango de IP, lo que implica tener menos control sobre parte del tráfico que se envía a endpoints con la misma IP de referencia

## Sobre Cloud NAT

Es un servicio administrado distribuido definido por software. No se basa en dispositivos o máquinas virtuales proxy.

Cloud NAT configura el software de Andrómeda que alimenta nuestra VPC para que proporcione traducción de direcciones de red de origen (NAT de origen o SNAT) para máquinas virtuales sin direcciones IP externas. También proporciona traducción de direcciones de red de destino (NAT de destino o DNAT) para paquetes de respuesta entrantes establecidos.

### Beneficios

**Seguridad**

Puede reducir la necesidad de máquinas virtuales individuales para que cada una tenga direcciones IP externas. Sujeto a las reglas del firewall de salida, las VM sin direcciones IP externas pueden acceder a destinos en Internet. Por ejemplo, es posible que tenga máquinas virtuales que solo necesiten acceso a Internet para descargar actualizaciones o completar el aprovisionamiento.

**Disponibilidad**

Cloud NAT es un servicio administrado distribuido definido por software. No depende de ninguna máquina virtual en su proyecto o de un solo dispositivo de puerta de enlace físico. Configura una puerta de enlace NAT en un Cloud Router, que proporciona el plano de control para NAT y contiene los parámetros de configuración que usted especifica. Google Cloud ejecuta y mantiene procesos en las máquinas físicas que ejecutan sus VM de Google Cloud.

**Escalabilidad**

Cloud NAT se puede configurar para escalar automáticamente la cantidad de direcciones IP de NAT que usa, y admite VM que pertenecen a grupos de instancias administrados, incluidos aquellos con ajuste de escala automático habilitado.

**Rendimiento**

Cloud NAT no reduce el ancho de banda de la red por VM. Cloud NAT es implementado por la red definida por software Andromeda de Google.

*Una VPC esta asociada a un proyecto, por lo tanto, si tu tienes varios proyectos, vas a necesitar definir diferentes VPCs, si cada uno de estos proyectos esta asociado a un diferente equipo de trabajo en cada equipo de trabajo* ***vamos a necesitar tener a una persona*** *que tenga el conocimiento de la gestión y configuración de las VPCs para que pueda hacer lo correspondiente en cada proyecto …*

SHARED VPC

Tiene definidos todos los recursos, reglas de firewall, diferentes subredes. Rangos de ip. Etc.

# Descripción general del intercambio de tráfico entre redes de VPC

<https://cloud.google.com/vpc/docs/vpc-peering>

INTRODUCCIÓN A COMPUTE ENGINE

Servicios de cómputo en la nube debe de ser un servicio bajo demanda/autoservicio, poder entrar a un navegador a la página del proveedor y consumir los recursos que se necesitan.  
Todo el acceso a servicios de nube deben ser a través de una red, típicamente internet.  
Los servicios físicos del proveedor de nube se comparten entre sus clientes.  
La elasticidad, para incrementar la capacidad de cómputo de las aplicaciones, es rápida.  
El pago es solamente por lo que se usa.

Compute Engine (Infraestructura como Servicio)

* Máquinas Virtuales (VMs) de propósito general y optimizadas
* Preemptible VMs (máquina virtual encendida máxima 24 horas, puede apagarse antes, la ventaja es que generan ahorro de costo significativo)
* Pago por segundo / Descuentos por uso sostenidos
* Migración en caliente (Live Migration)
* Recomendaciones de dimensionamiento
* Tipos de máquinas predefinidas y personalizables

## Familias de máquinas virtuales

### Propósito general

#### Efficient E2

* Optimización costo
* Ahorro es prioridad

#### Balanced N2, N2D

* Balanceadas
* Desempeño y TCO (Total Cost of Ownership)

#### TAU T2D

* Optimizado para escalabilidad
* Desempeño alta escalabilidad

### Cargas de trabajo optimizadas

#### C2

* Optimización computo
* Mejor desempeño de CPUs

#### M1 M2

* Optimización Memoria
* Mayor memoria

#### A2

* Optimización Aceleración
* GPUs del más alto desempeño

### Máquinas virtuales personalizables

Crear tus propias configuraciones de máquina virtual.