VPC

It stands for Virtual Private Network.

VPC is a private network inside Google Cloud. It is a virtual version of a real physical network, and it helps different parts of cloud setup to talk to each other securely.

It performs many functions like connecting VM instances to other Google cloud services built on VMs. It helps distribute traffic and supports load balancers.

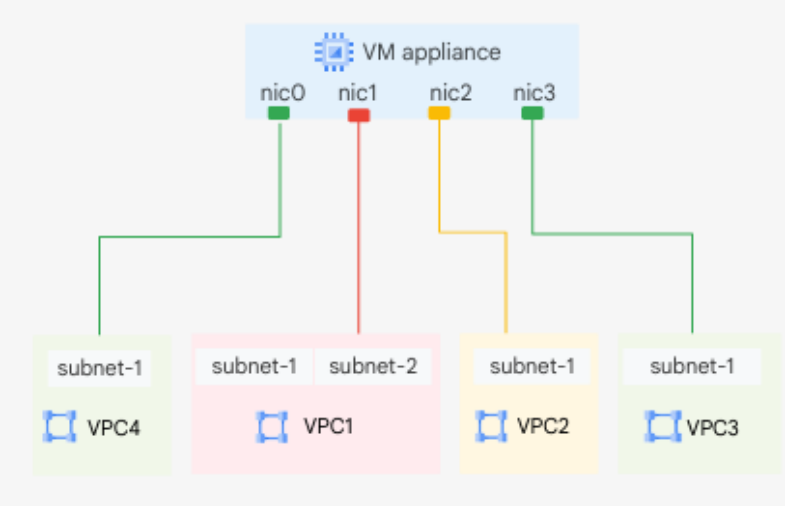
New project starts with a default network (an auto mode VPC network) that has one subnet in each region, so that VMs can be deployed directly.

Multiple Network Interfaces

MNIs help in designing a secure and efficient network architecture.

They are helpful when an organization requires a secure virtual appliance which can handle tasks like load balancing, intrusion detection/prevention (IDS/IPS), and web application firewalls (WAF).

They separate the traffic, one interface for data traffic and another one for management traffic.



Each NIC is attached to a separate VPC network and uses an internal IP to communicate across networks.

You cannot add or remove NICs once an instance is created. If you want to do so, then delete entire instance.

Each interface must be in a different network and network IP ranges cannot overlap.

The networks must exist before you create the VM.

VM-Instance-A has *nic0* in VPC-A, and VM-Instance-B is in VPC-B.

If you access *VM-Instance-B.internal* from *VM-Instance-A* then DNS resolver of *VM-Instance-A* could not resolve it because *VM-Instance-B*'s internal DNS name is valid in context of VPC-B.

NIC Limit

Type of instance	Maximum virtual NICs
VM <= 2 vCPU	2 NICs
VM > 2 vCPU	1 NIC per vCPU (Max: 8)

Network Service Tiers

1. Premium Tier (↑ cost, ↑ performance)
   Traffic passes through Google's private global fiber network.
   Performance is main consideration.
   Traffic enters the nearest PoP (Point of Presence) to user, means traffic travels less over Internet.
   Provides low latency, high speed and better performance.
2. Standard Tier (↓ cost, ↓ performance)
   Traffic travels over public network (Internet).
   Cost is main consideration.
   Google's network is less used, implies less cost.
   Increment in latency and inconsistent performance.
   Traffic chooses standard route results in low costs but also lower quality.

Mini Project

1. Create custom mode VPC network with firewall rules
   a. In the Cloud console, click **Activate Cloud Shell.**
   b. If prompted, click Continue, then run the command to create the privatenet network:

```
gcloud compute networks create privatenet --subnet-mode=custom
```

   c. Run the command to create a subnet privatesubnet-s:

```
gcloud compute networks subnets create privatesubnet-s --network=privatenet --region=us-central1 --range=172.16.0.0/24
```

   d. Run the command to create a subnet privatesunet-t:

```
gcloud compute networks subnets create privatesubnet-t --network=privatenet --region=europe-west1 --range=172.20.0.0/20
```

   e. Run the command to list the available VPC networks:

```
gcloud compute networks list
```

2. Create the firewall rules
   a. Run the command to create the privatenet-allow-icmp-ssh-rdp firewall rule:

gcloud compute firewall-rules create privatenet-allow-icmp-ssh-rdp --direction=INGRESS --priority=1000 --network=privatenet --action=ALLOW --rules=icmp,tcp:22,tcp:3389 --source-ranges=0.0.0.0/0

The output should look like this:

```
NAME: privatenet-allow-icmp-ssh-rdp
NETWORK: privatenet
DIRECTION: INGRESS
PRIORITY: 1000
ALLOW: icmp,tcp:22,tcp:3389
DENY:
DISABLED: False
```

3. Run the command to create the privatenet-s-vm instance:

gcloud compute instances create privatenet-s-vm --zone=us-central1-f --machine-type=e2-medium --subnet=privatesubnet-s

4. In the same fashion, create another custom mode VPC network (managementnet) with firewall rules, VM instances (managementnet-s-vm).
5. You can ping the external IP address of all VM instances, even though they are in either a different zone or VPC network. This confirms that public access to those instances is only controlled by the **ICMP** firewall rules that you established earlier.
6. No internal IP address communication is allowed between networks, unless you set up mechanisms such as VPC peering or VPN.
7. Create a VM instance with multiple network interfaces
   a. In the Cloud console, in the Navigation menu, click Compute Engine >> VM instances.
   b. Fill the following, and leave the remaining settings as their defaults:
      Name: vm-appliance
      Region: us-central1
      Zone: us-central1-c
   c. Choose Machine configuration: Series: E2 | Machine type: 4vCPUs (16 GB memory, e2-standard-4)
   d. Select Networking and add Network interfaces (privatenet, managementnet)
   e. For vm-appliance, click SSH and run the command to list the network interfaces within the VM instance:

sudo ifconfig

   f. Explore the network interface connectivity by pinging from vm-appliance's SSH terminal to internal IPs' of created VMs.