



GCP Networking

Google Cloud

By Vishal Bulbule
Google Cloud Champion Innovator
Fully Certified in Google Cloud

Cloud Networking

- IP Address
- Virtual Private Cloud (VPC)
- Subnet
- CIDR range
- Firewalls
- NAT Gateway
- Identity-aware proxy
- VPC Peering
- Shared VPC

IP Address

IP addresses contain 4 octets, each consisting of 8 bits giving values between 0 and 255.

The decimal value that comes after the slash is the number of bits consisting of the routing prefix.

This in turn can be translated into a netmask, and also designates how many available addresses are in the block.

10 . 88 . 135 . 144 / 28

0 0 0 0 1 0 1 0

255.255.255.240
NETMASK

0 1 0 1 1 0 0 0

10.88.135.145
FIRST USABLE IP

1 0 0 0 0 1 1 1

10.88.135.158
LAST USABLE IP

1 0 0 1 0 0 0 0

16
COUNT

Private IP vs Public IP

Private IP	Public IP
Used with LAN or Network	Used on Public Network
Not recognized over Internet	Recognized over Internet
Assigned by LAN administrator	Assigned by Service provider / IANA
Unique only in LAN	Unique Globally
Free of charge	Cost associated with using Public IP
Range – Class A -10.0.0.0 to 10.255.255.255 Class B – 172.16.0.0 to 172.31.255.255 Class C – 192.168.0.0 – 192.168.255.255	Range – Class A -1.0.0.0 to 9.255.255.255 11.0.0.0 – 126.255.255.255 Class B -128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255 Class C -192.0.0.0 – 192.167.255.255 192.169.0.0 to 223.255.255.255

Virtual Private Cloud (VPC)

A Virtual Private Cloud (VPC) network is a virtual version of a physical network, implemented inside of Google's production network, using Andromeda. A VPC network provides the following:


- Provides connectivity for your Compute Engine virtual machine (VM) instances, including Google Kubernetes Engine (GKE) clusters, App Engine flexible environment instances, and other Google Cloud products built on Compute Engine VMs.
- Offers native Internal TCP/UDP Load Balancing and proxy systems for Internal HTTP(S) Load Balancing.
- Connects to on-premises networks using Cloud VPN tunnels and Cloud Interconnect attachments.
- Distributes traffic from Google Cloud external load balancers to backends.
- A network must have at least one subnet before you can use it. Auto mode VPC networks create subnets in each region automatically.

Subnet

Virtual Private Cloud (VPC) networks are global resources. Each VPC network consists of one or more IP address range called subnets. Subnets are regional resources, and have IP address ranges associated with them.

Valid IPv4 ranges

A subnet's primary and secondary IPv4 address ranges are regional internal IPv4 addresses. The following table describes valid ranges.

Range	Description
Private IPv4 address ranges	
10.0.0.0/8	Private IP addresses RFC 1918 
172.16.0.0/12	
192.168.0.0/16	

CIDR Ranges

What is CIDR address range?

Classless Inter-Domain Routing (CIDR) is a range of IP addresses a network uses. A CIDR address looks like a normal IP address, except that it ends with a slash followed by a number. The number after the slash represents the number of addresses in the range. Here's an example CIDR IP address in IPv4: 192.0.2.0/24

192.0.2.0/28 - $(32-28=4) \rightarrow 2^4 = 16$ IP addresses

192.0.2.0/24 - $(32-24=8) \rightarrow 2^8 = 256$ IP addresses

VPC Firewalls

Virtual Private Cloud (VPC) firewall rules apply to a given **project** and **network**.

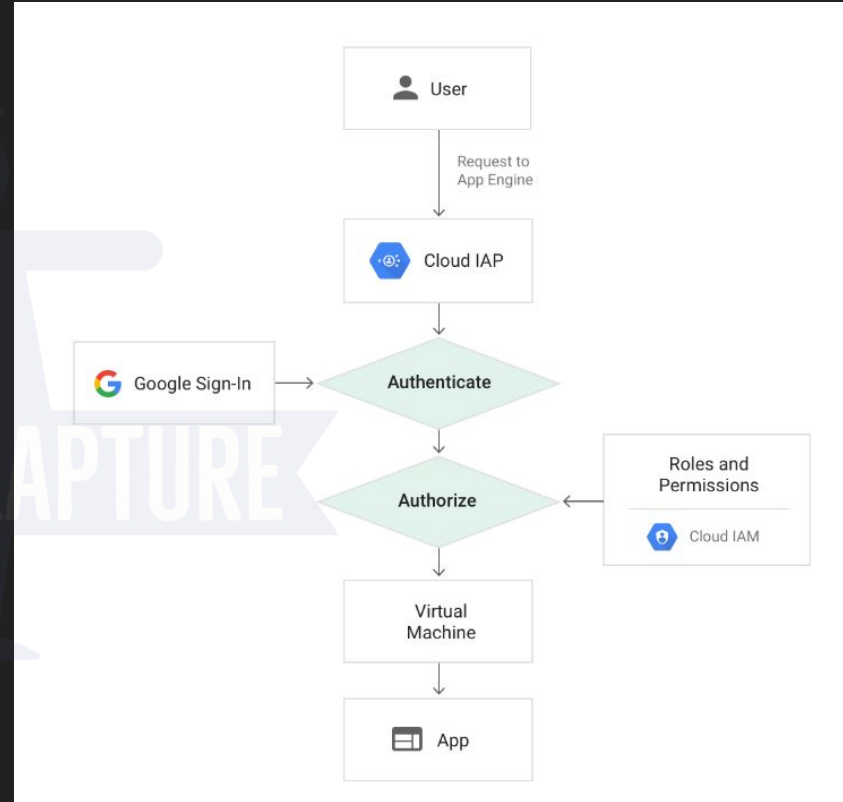
If you want to apply firewall rules to multiple VPC networks in an organization, see **Firewall Policies**.

VPC firewall rules let you **allow** or **deny** connections to or from your virtual machine (VM) instances based on a configuration that you specify.

Enabled VPC firewall rules are always enforced, protecting your instances regardless of their configuration and operating system, even if they have not started up.

Identity-Aware Proxy

Identity-Aware proxy (IAP) to login into GCE instance without public/external IP. Identity-Aware Proxy (IAP) TCP forwarding to enable administrative access to VM instances that do not have external IP addresses or do not permit direct access over the internet



How to enable IAP

To enable IAP we need to -

- 1) Enable **Cloud Identity Aware Proxy** API
- 2) Assign **roles/iap.tunnelResourceAccessor** role to the user
- 3) Create firewall to allow ssh traffic from IP range

35.235.240.0/20 this is fixed IP range provided by google.



Cloud Identity-Aware Proxy API

Google Enterprise API ?

Controls access to cloud applications running on Google Cloud Platform.

Cloud NAT

Cloud NAT (**network address translation**) lets certain resources without external IP addresses create outbound connections to the internet.

Cloud NAT provides outgoing connectivity for the following resources:

- Compute Engine virtual machine (VM) instances without external IP addresses
- Private Google Kubernetes Engine (GKE) clusters
- Cloud Run instances through Serverless VPC Access
- Cloud Functions instances through Serverless VPC Access
- App Engine standard environment instances through Serverless VPC Access

Cloud NAT

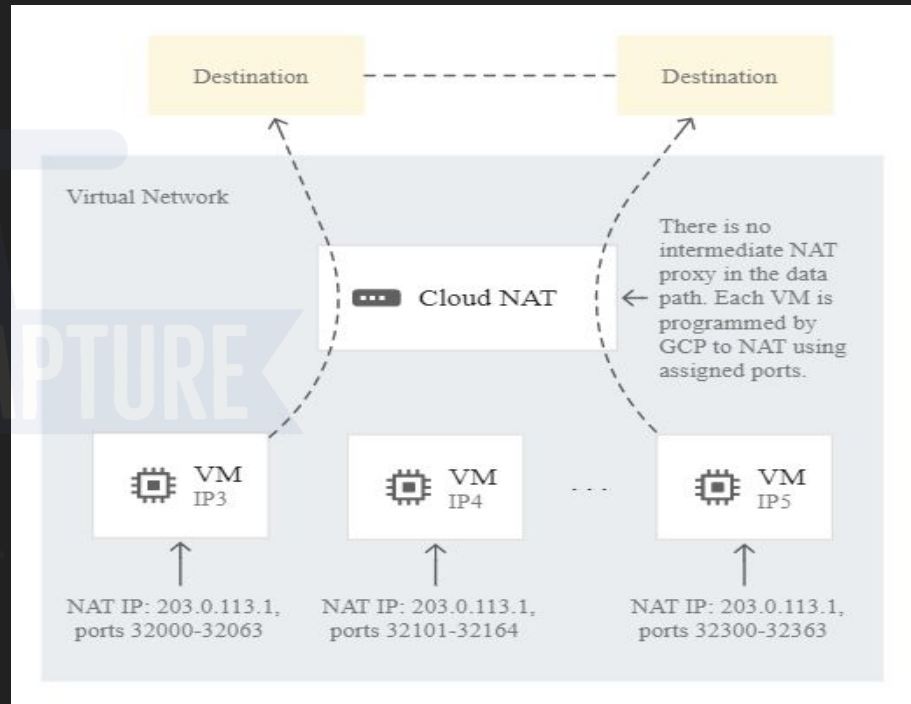


NAT IP addresses

A NAT IP address is a regional external IP address, routable on the internet. A VM without an external IP address, in a subnetwork (subnet) served by a Cloud NAT gateway, uses a NAT IP address when it sends packets to a destination on the internet.

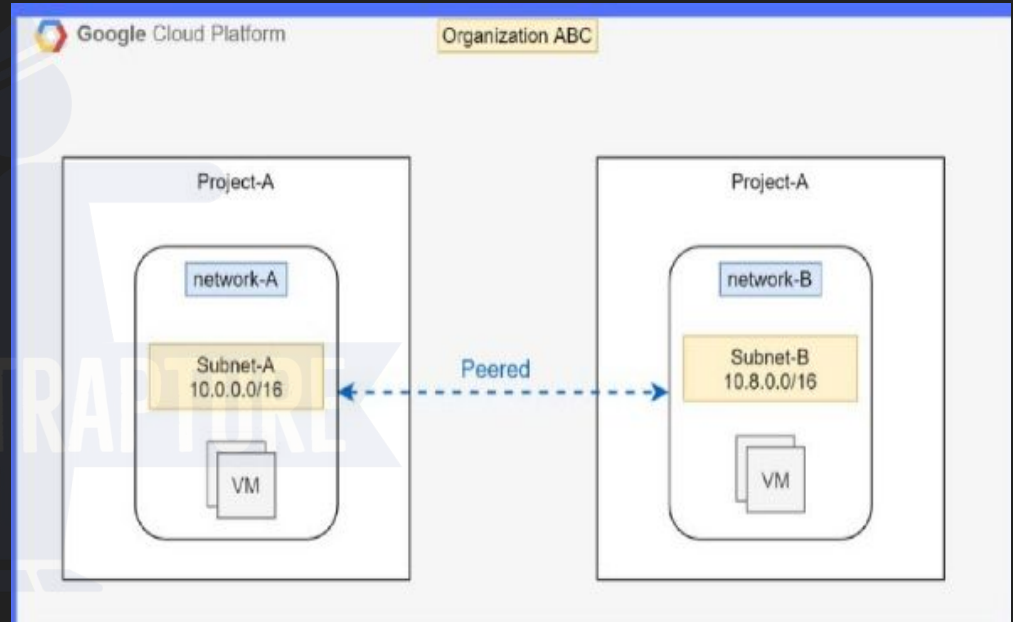
Ports

Each NAT IP address on a Cloud NAT gateway offers 64,512 TCP source ports and 64,512 UDP source ports. TCP and UDP each support 65,536 ports per IP address, but Cloud NAT doesn't use the first 1,024 well-known (privileged) ports.



VPC Peering

- Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.
- VPC Network Peering enables you to connect VPC networks so that workloads in different VPC networks can communicate internally. Traffic stays within Google's network and doesn't traverse the public internet.



VPC Peering - Advantages

VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks, including:

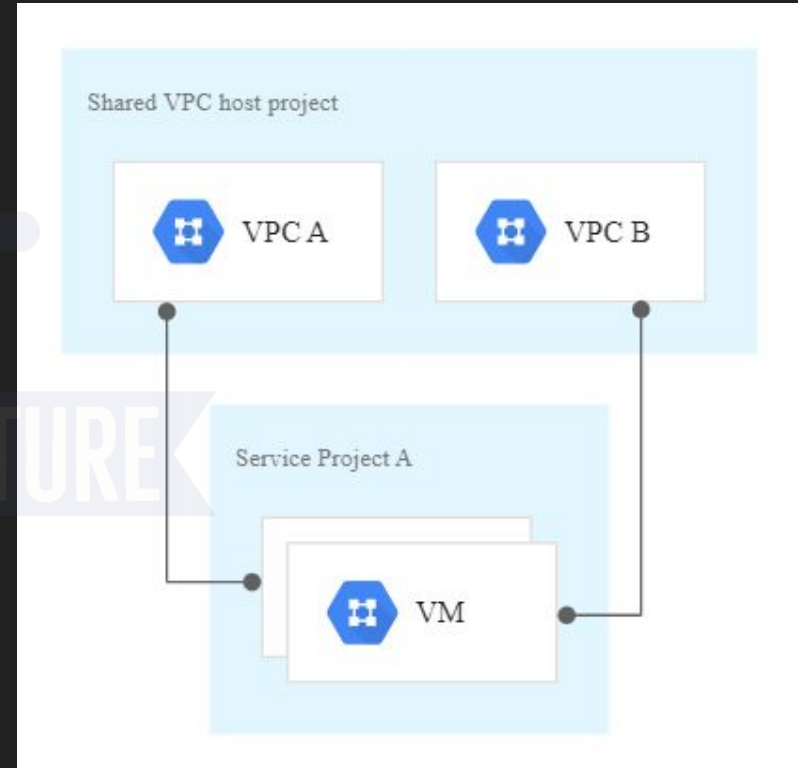
Network Latency: Connectivity that uses only internal addresses provides lower latency than connectivity that uses external addresses.

Network Security: Service owners do not need to have their services exposed to the public Internet and deal with its associated risks.

Network Cost: Google Cloud charges egress bandwidth pricing for networks using external IPs to communicate even if the traffic is within the same zone. If however, the networks are peered they can use internal IPs to communicate and save on those egress costs. Regular network pricing still applies to all traffic.

Shared VPC

- Shared VPC allows an organization to connect resources from multiple projects to a common Virtual Private Cloud (VPC) network, so that they can communicate with each other securely and efficiently using internal IPs from that network.
- When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it. The VPC networks in the host project are called Shared VPC networks.
- Eligible resources from service projects can use subnets in the Shared VPC network.



Shared VPC reference Architecture

