WHAT IS GOOGLE CLOUD VPC?

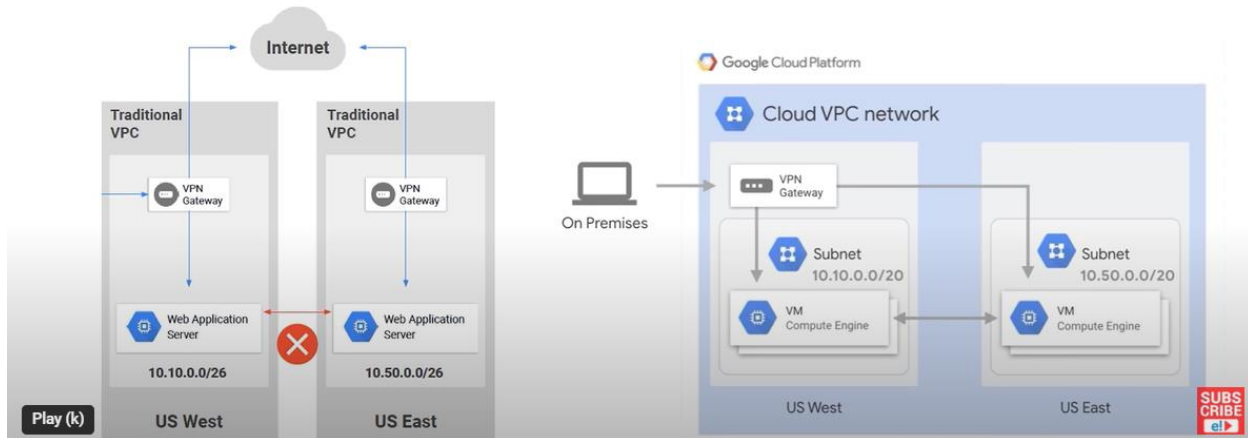# WHAT IS GOOGLE CLOUD VPC?
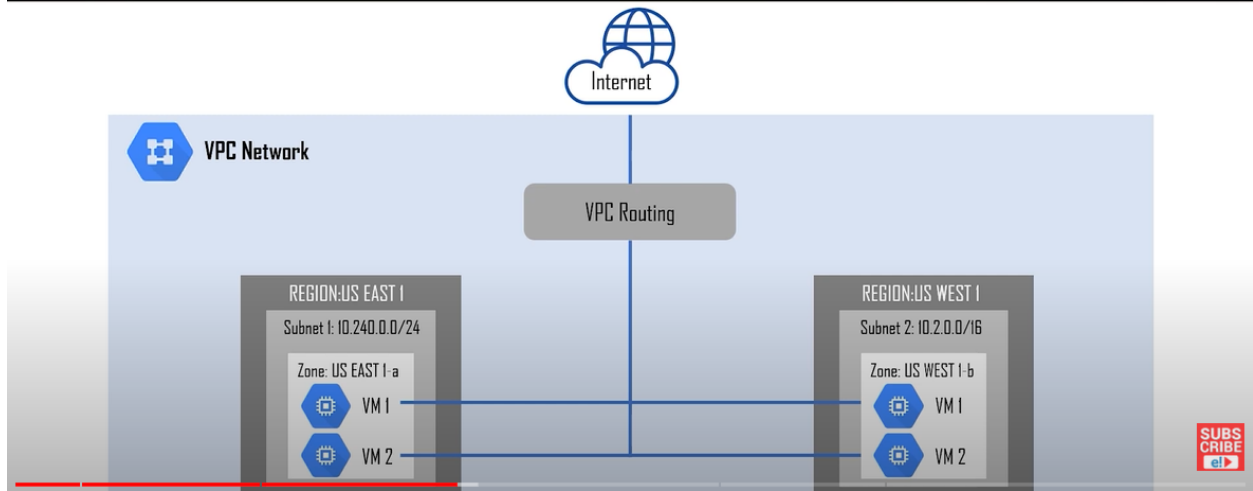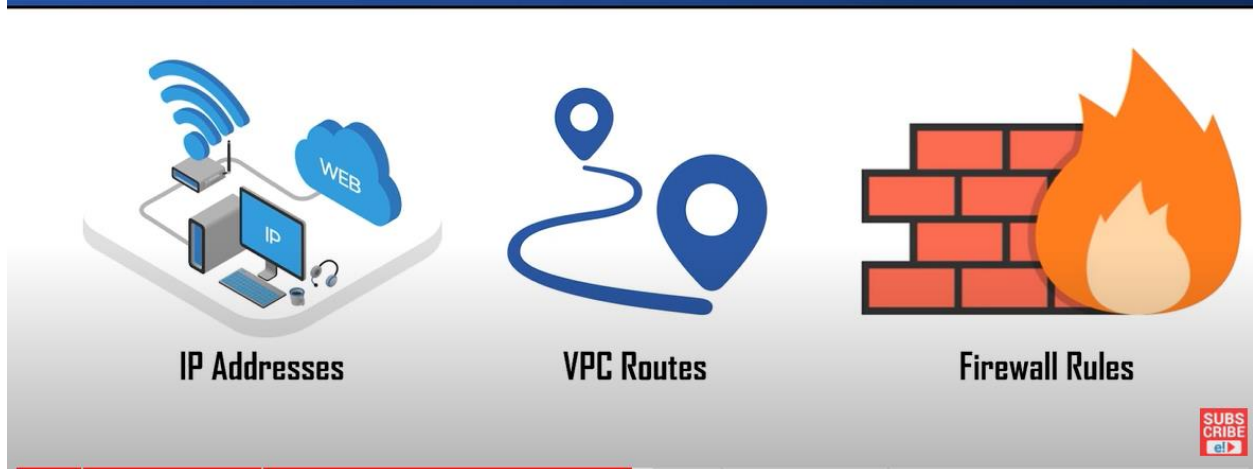
WHAT IS GOOGLE CLOUD VPC?

VPC Network

✓ It Provides connectivity for your Compute Engine virtual machine(VM) instances.

✓ It offers built-in Internal TCP/UDP Load Balancing and proxy systems for Internal HTTP(S) Load Balancing.

• It connects to on-premises networks using Cloud VPN tunnels and Cloud Interconnect attachments.

• Distributes traffic from Google Cloud external load balancers to backends.

WHAT IS GOOGLE CLOUD VPC?

Internet

VPC Network

VPC Routing

REGION:US EAST 1
Subnet 1: 10.240.0.0/24

Zone: US EAST 1-a
VM 1
VM 2

REGION:US WEST 1
Subnet 2: 10.2.0.0/16

Zone: US WEST 1-b
VM 1
VM 2

WHAT IS GOOGLE CLOUD VPC?

WEB
IP

IP Addresses

VPC Routes

Firewall Rules

BENEFITS OF GOOGLE CLOUD VPC

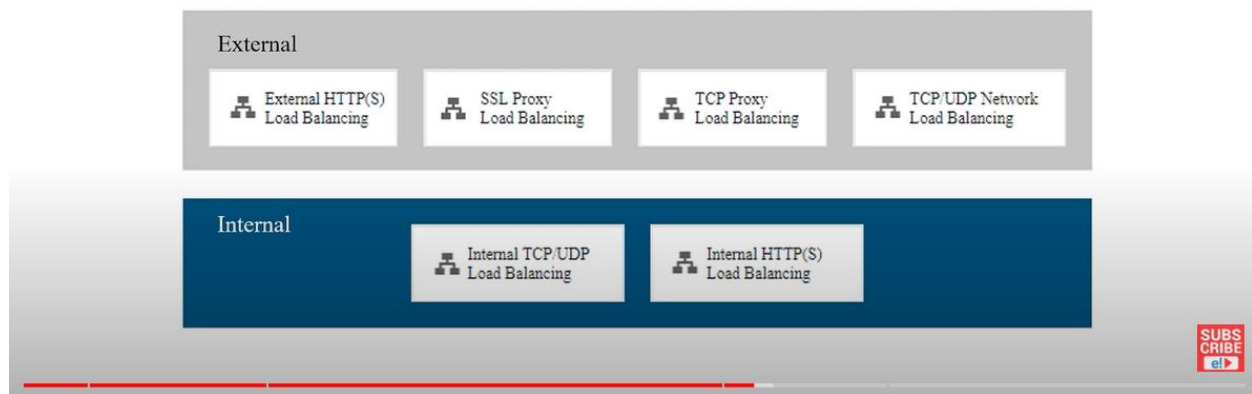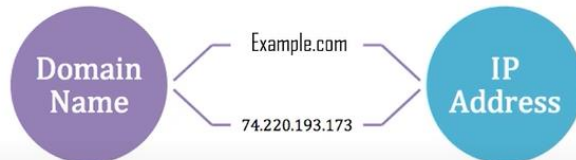| Global	Shareable	Expandable
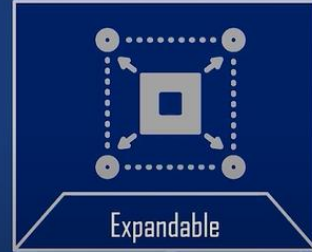
OVERVIEW OF OTHER GCP NETWORKING CONCEPTS

A **Load Balancer** distributes user traffic across multiple instances of your applications by spreading the load

OVERVIEW OF OTHER GCP NETWORKING CONCEPTS

OVERVIEW OF OTHER GCP NETWORKING CONCEPTS

Google Cloud provides a Scalable, reliable, and managed **Domain Name service** or **DNS** running on the same infrastructure as Google

- **Virtual Private Cloud**
  - Region, Zones, Subnet, Routes & Firewall Rules
  - VPC Peering
  - Shared VPC

- **Load Balancing**
  - Global Load Balancer (HTTP(s) Load Balancer, SSL Proxy, TCP Proxy)
  - Regional Load Balancer (Network TCP/UDP, Internal TCP/UDP)

Every location or device on a network must be <u>addressable</u>. In the TCP/IP model of network layering, it's referred as IP address.

Network Address Translation allows the addresses to be rewritten when packets traverse network borders to allow them to continue to their correct destination.

IPv4 - Four octets, 32 bit address, Each 8-bit segment is divided by a period and typically expressed as a number 0-255. ex- 192.168.20.10
IPv6 – 16 bit blocks, 128 bit address, 8 segments of four hexadecimal digits, double colon (::) is used for leading zeros. ex -
1203:8fe0:fe80:b897:8990:8a7c:99bf:323d

IPv4

An IPv4 address (dotted-decimal notation)

172 . 16 . 254 . 1

10101100 .00010000 .11111110 .00000001

One byte = Eight bits

Thirty-two bits (4 x 8), or 4 bytes
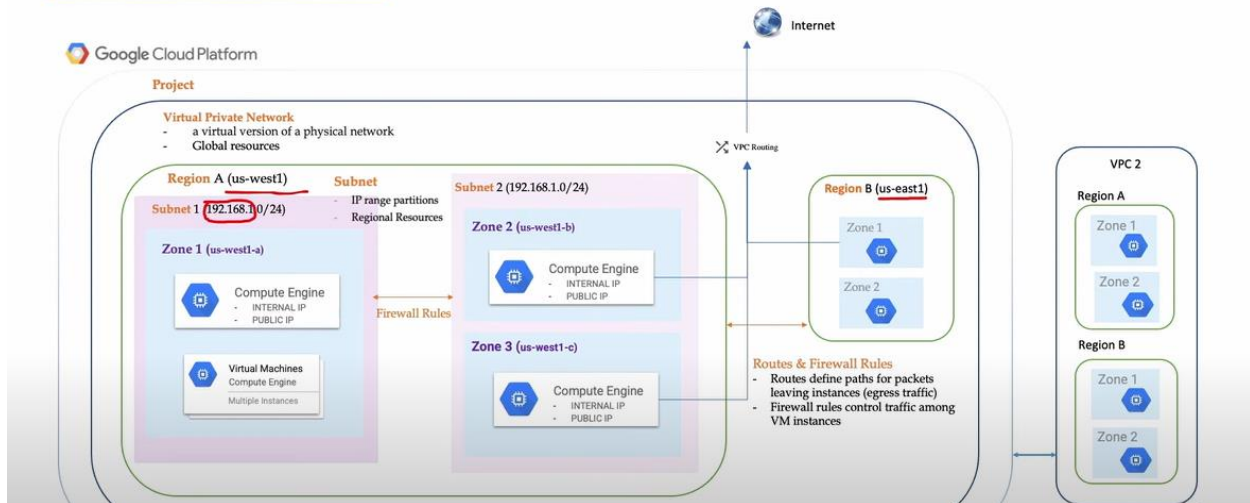
IPv6

An IPv6 address   (in hexadecimal)

2001:0DB8:AC10:FE01:0000:0000:0000:0000
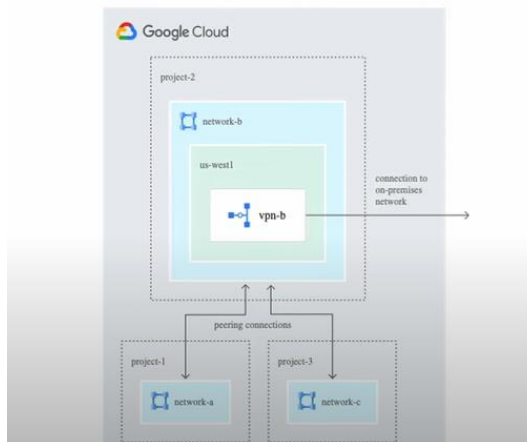
2001:0DB8:AC10:FE01::   Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:
0000000000000000:0000000000000000:0000000000000000:0000000000000000

VPC Network Peering enables you to connect VPC networks so that workloads in different VPC networks can communicate internally.

Specifications:

✓ 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.

✓ Traffic stays within Google's network and doesn't traverse the public internet.

✓ VPC Network Peering works with Compute Engine, GKE, and App Engine flexible environment.

✓ Peered VPC networks remain administratively separate. Routes, firewalls, VPNs, and other traffic management tools are administered and applied separately in each of the VPC networks.

✓ VPC Network Peering is useful in these environments:
   1. SaaS (Software-as-a-Service) ecosystems in Google Cloud
   2. Organizations with several network administrative domains

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

   1. Network Latency
   2. Network Security
   3. Network Cost (egress)

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.

Host Project

Shared VPC Network

A host project contains one or more Shared VPC networks.

Region (us-west1)

Subnet (10.0.1.0/24)

Compute Engine
- 10.0.1.3

Region (us-east1)

Subnet (10.15.2.0/24)

Compute Engine
- 10.15.2.4

A Shared VPC network is a VPC network defined in a host project and made available as a centrally shared network for eligible resources in service projects.
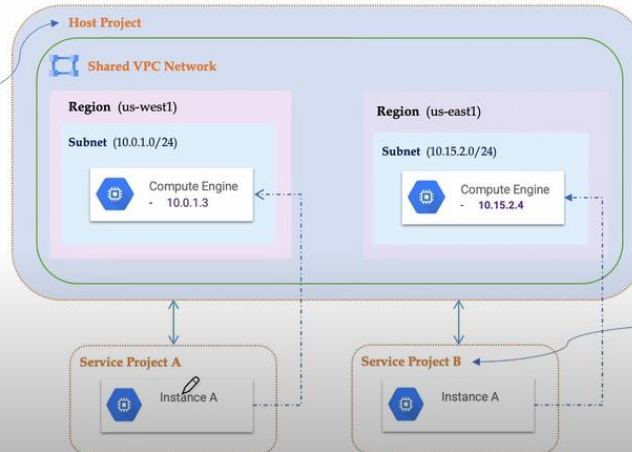
Project Requirements:
1. Delegate Administrative responsibilities for Networking
2. Hybrid Cloud & Transit Network

Service Project A

Instance A

Service Project B

Instance A

A service project is any project that has been attached to a host project by a Shared VPC Admin

---

Cloud Load Balancing is a fully distributed, software-defined managed service, which distributes user traffic across multiple instances of applications.

Backends
Compute Engine

Cloud Load Balancing

Backends
Cloud Storage

External — **Internal**

External HTTP(S) Load Balancing
SSL Proxy Load Balancing
TCP Proxy Load Balancing
TCP/UDP Network Load Balancing

Internal HTTP(S) Load Balancing
Internal TCP/UDP Load Balancing
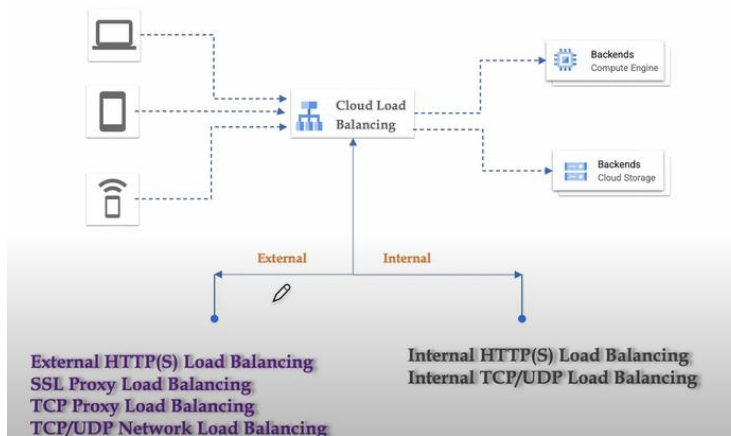
Google Cloud offers the following load balancing features:

- Single IP address to serve as the frontend
- Automatic intelligent autoscaling of the backends
- Layer 4-based load balancing to direct traffic based on data from network and transport layer protocols, such as IP address and TCP or UDP port
- Layer 7-based load balancing to add content-based routing decisions based on attributes, such as the HTTP header and the uniform resource identifier
- Integration with Cloud CDN for cached content delivery

The following diagram illustrates a common use case: how to use external and internal load balancing together.

Internal Tier with regional internal load balancing

HTTP(S) or TCP/UDP

Web Tier with external load balancing
Global: HTTP(S), SSL Proxy
Regional: Network TCP/UDP

us-central1-a

Web Tier

Internal Load Balancing
IP: 10.10.10.10, Port: 80

Internal Tier — Database Tier

User in San Francisco

External Load Balancing
IP: 1.1.1.1, Port: 80

Web Tier

Internal Tier — Database Tier

User in Iowa

us-central1-b

User in Singapore

asia-east1-a

Web Tier

Internal Load Balancing
IP: 10.20.1.1, Port: 80

Internal Tier — Database Tier

IPv6 Client — IPv4 Client

External
Internet -> GCP

Internal
Traffic to/from internal IP addresses

Internal IPv4 Client

HTTP(S) Traffic — TCP Traffic — UDP Traffic — External Network Load Balancing — TCP Traffic — UDP Traffic — HTTP(S) Traffic

SSL offload? — No

Global LB or IPv6? — No

Preserve Client IPs

Yes — Yes — No — Yes

HTTP(S) Load Balancing — SSL Proxy — TCP Proxy — External Network Load Balancing — Internal TCP/UDP Load Balancing — Internal HTTP(S) Load Balancing

- **Network address translation (NAT)** is a method of remapping one IP address space into another by modifying network address information in the IP header of packet. Usually this is done in a NAT device.

- **IP masquerading or Network address Translation** is a technique that hides an entire IP address , usually the private IP addresses, behind a single IP address usually the public address. The hidden addresses are changed into a single (public) IP address as the source address of the outgoing IP packets so they appear as originating from the routing device and not from the hidden host.
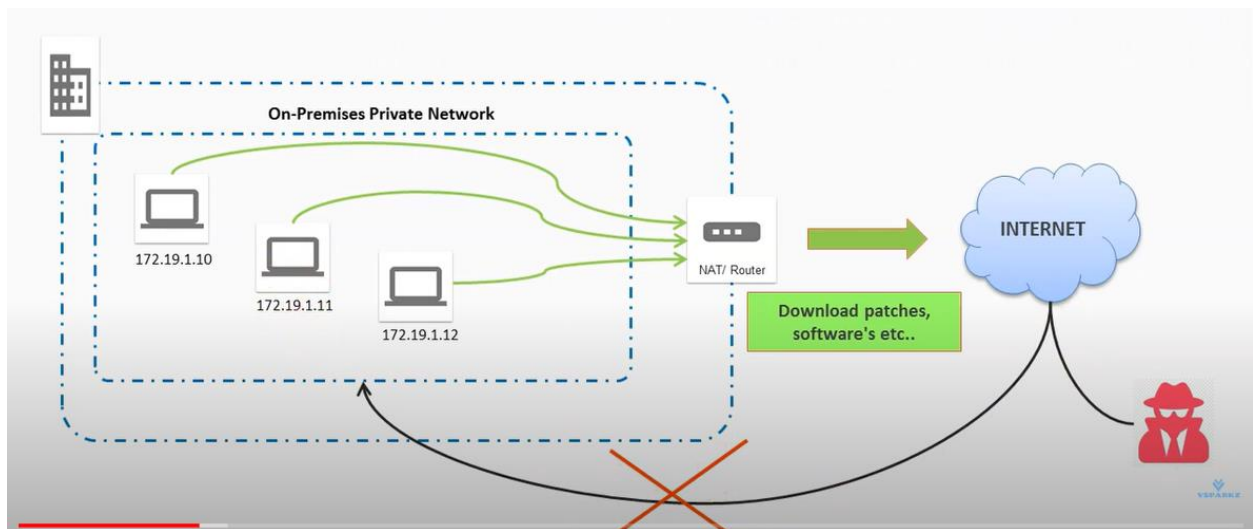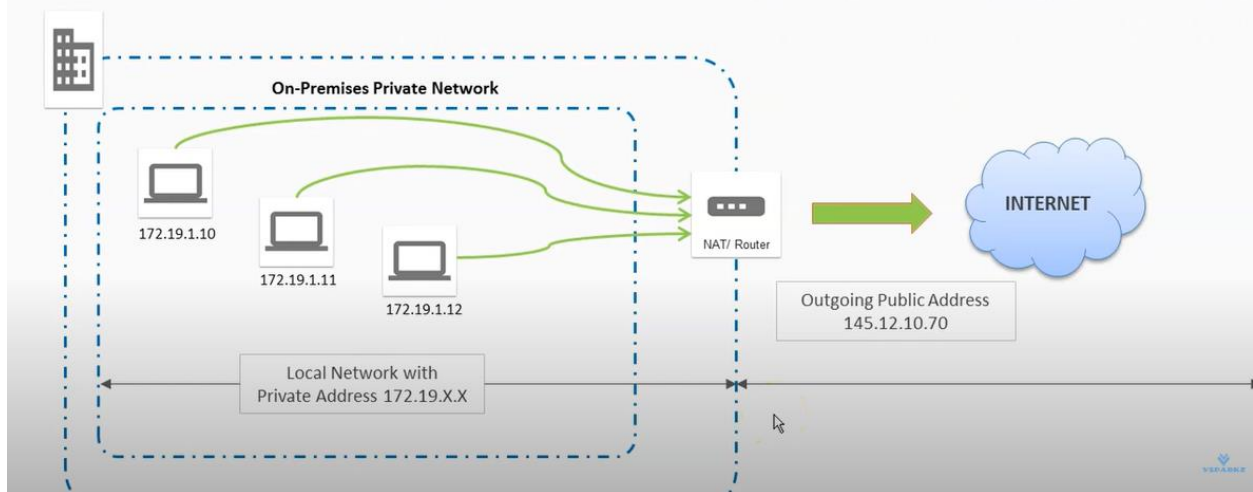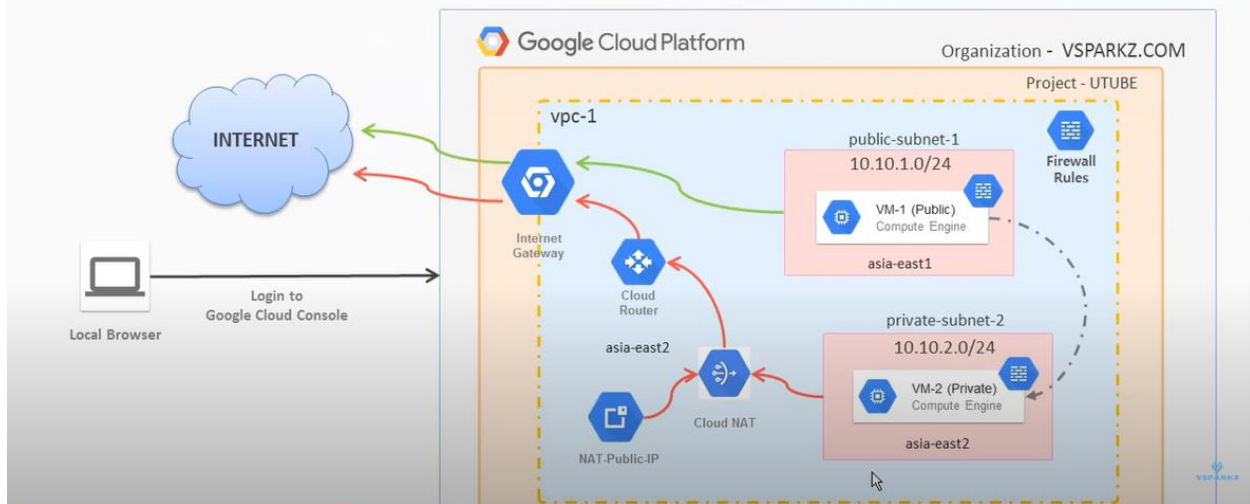
In which scenario do we use the CLOUD NAT in the GCP project?

There are many scenarios where using cloud NAT in a GCP project, like

- Securely connecting private instances to the internet
- Connecting to on-premises resources
- Connecting instances across VPCs
- Scalable outbound traffic management
- Cost-effective solution for managing public IP

Benefits of Cloud NAT:

- Improved security
- Reduced costs
- Simplified management
- Scalability

What is Google 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

Benefits

- Security
  - You can reduce the need for individual VMs to each have external IP addresses.
- Availability
  - Cloud NAT is a distributed, software-defined managed service. It doesn't depend on any VMs in your project or a single physical gateway device. You configure a NAT gateway on a Cloud Router, which provides the control plane for NAT, holding configuration parameters that you specify. Google Cloud runs and maintains processes on the physical machines that run your Google Cloud VMs.
- Scalability
  - Cloud NAT can be configured to automatically scale the number of NAT IP addresses that it uses, and it supports VMs that belong to managed instance groups, including those with autoscaling enabled.
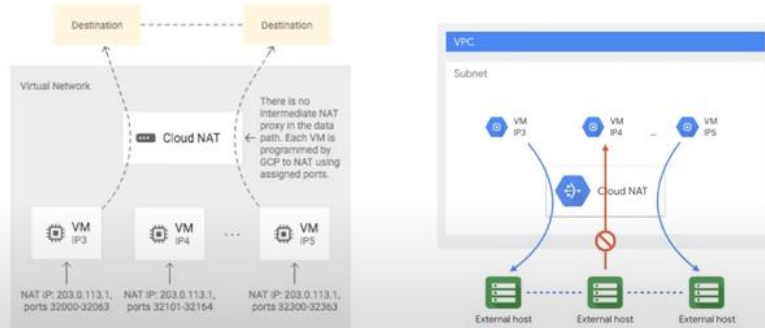
Cloud NAT

- Cloud NAT **(network address translation)** lets certain resources without external IP addresses create outbound connections to the internet.
- It's a way to map multiple local private addresses to a public one before transferring the information

Demo

- How to create Cloud NAT Gateway

Cloud NAT

#GCPSketchnote

@PVERGADIA THECLOUDGIRL.DEV 7.14.2021

What is Cloud NAT??

NETWORK ADDRESS TRANSLATION

PROVIDES OUTGOING CONNECTIVITY TO RESOURCES WITHOUT EXTERNAL IP

Serverless VPC Access Connector

CLOUD NAT BENEFITS

- Security
- Availability
- Scalability
- Performance

BASIC CLOUD NAT CONFIGURATION EXAMPLES

Update Service
203.0.113.1

Internet

NAT gateway is per region of each network

us-east1

NAT-GW-US-EAST — NAT IPs 192.0.2.50, 192.0.2.60

Subnet 1 | Subnet 2

Zone A
10.240.0.2
10.240.0.3

Cannot access internet

Can access internet via NAT gateway US

Zone B
10.240.0.2

172.16.1.2

europe-west1

NAT-GW-EU — NAT IPs 198.51.100.1

NAT gateway translates internal IP addresses to NAT IP addresses

Subnet 3

Zone C
192.168.1.2
192.168.1.3

Can access internet via NAT gateway EU

GCP Project

Update Service
203.0.113.0

Internet

VPC Network

Region: us-east1 — NAT Gateway US-East
NAT IPs 198.51.100.50 198.51.100.60

Subnet 1

VM Instance

Pod 1
IP: 10.0.1.1
(Configured as alias IPs)

Pod 2
IP: 10.0.1.2
(Configured as alias IPs)

Instance primary IP: 10.240.0.2
Secondary range: 10.0.1.0/24

Primary IP range: 10.240.0.0/24
Secondary IP range: 10.0.0.0/16

Cloud NAT with GKE

HOW IS CLOUD NAT DIFFERENT FROM TYPICAL NAT PROXIES?

Destination — Destination

Network NAT IP: 203.0.113.1

Physical dataplane hop → NAT Proxy

VM IP3 — VM IP4 — VM IP5

1. Typical NAT Proxies

Destination — Destination

Virtual Network

Logical NAT Gateway → Cloud NAT

There is no intermediate NAT proxy in the data path. Each VM is programmed by GCP to NAT using assigned ports.

VM IP3 — VM IP4 — VM IP5

NAT IP: 203.0.113.1 ports 32000-32063
NAT IP: 203.0.113.1 ports 32101-32164
NAT IP: 203.0.113.1 ports 32300-32363

2. Google Cloud NAT