GCP

Google Cloud

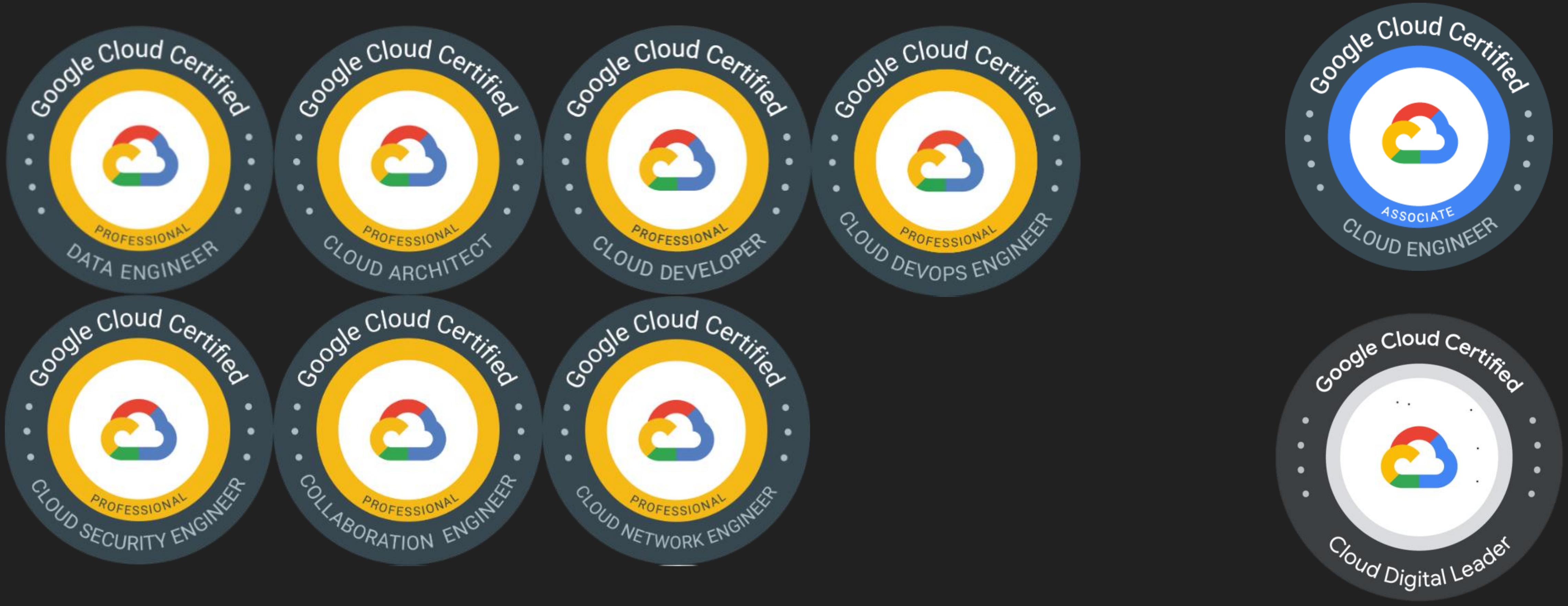
Professional Network Engineer

Google Certified Professional Cloud Network Engineer

Professional Network Engineer

- Pay attention for 5 minutes, before we dive in.
- Challenging certification, and course is long so have patience.
- Good to have basic IT skill & GCP basics
  - Basics of compute engine
- Learn by Doing

GCP certifications



https://cloud.google.com/certification/cloud-network-engineer

Cloud Cost for this course

- $0 – for GCP account
- GCP Free trial
- $300 for next 3 months https://cloud.google.com/free
- Length: Two hours
- Registration fee: $200 (plus tax where applicable)
- Languages: English, Japanese, Spanish.
- Exam format: Multiple choice and multiple select,

GCP Network Engineering

BY ANKIT MISTRY

Udemy Tips

BY ANKIT MISTRY

GCP Basics

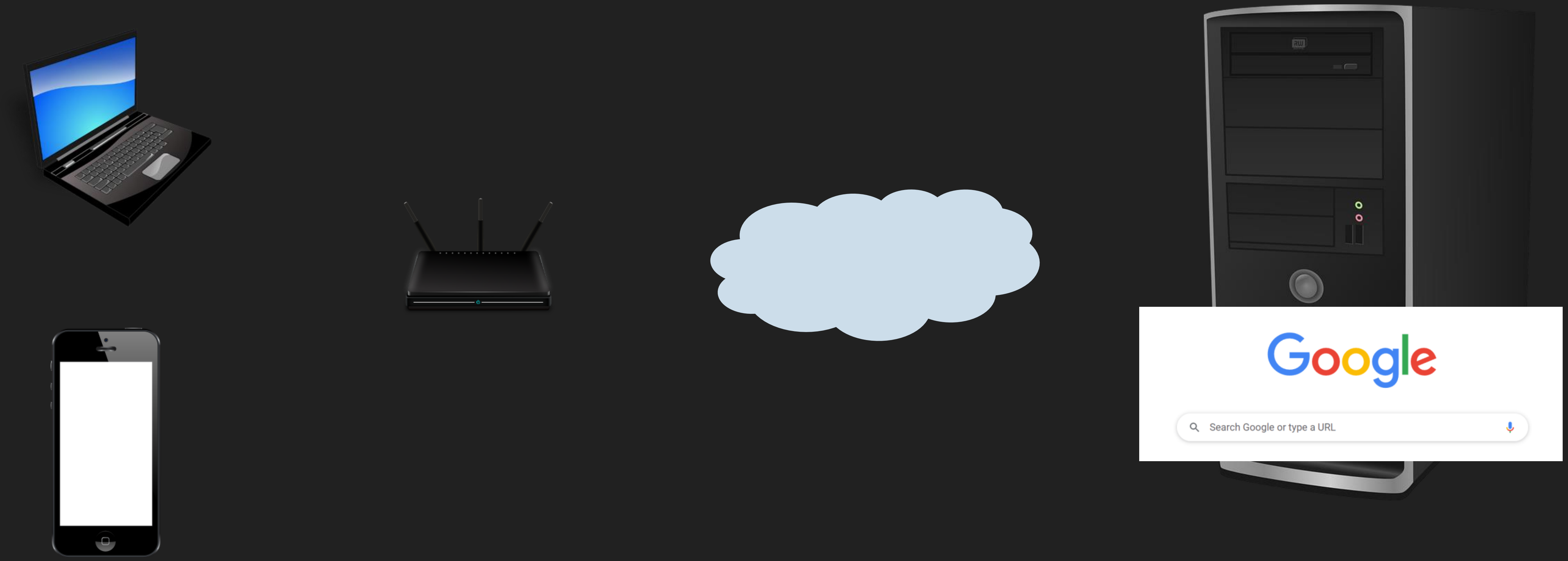
- Google Cloud Overview
- Create GCP Account
- GCP Console Walkthrough
- GCP Regions & Zones
- Creating GCP Project
- Google Cloud Shell

Networking Basics

- What is Network
- IP Address & CIDR ranges
- RFC 1918 standard

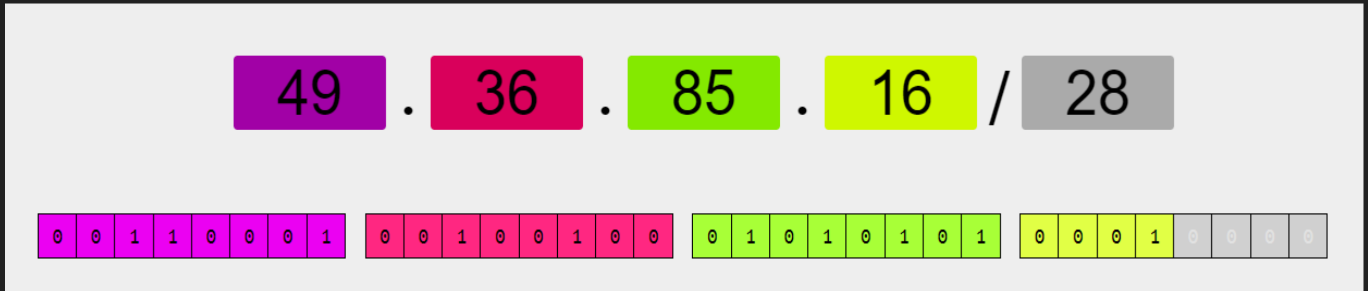
Network

Home Network



IP address

49.36.84.16



49 . 36 . 85 . 16 / 28

0	0	1	1	0	0	0	1	0	0	1	0	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	0	0	0

- 32 Bit representation
- IPV4 - 4 number
- 4 Billion address can be represented
- Advanced – IPV6
- many more IP can be represented – 2^128
- Your machine IP : https://api.ipify.org/

Ref : https://cidr.xyz/

CIDR notation

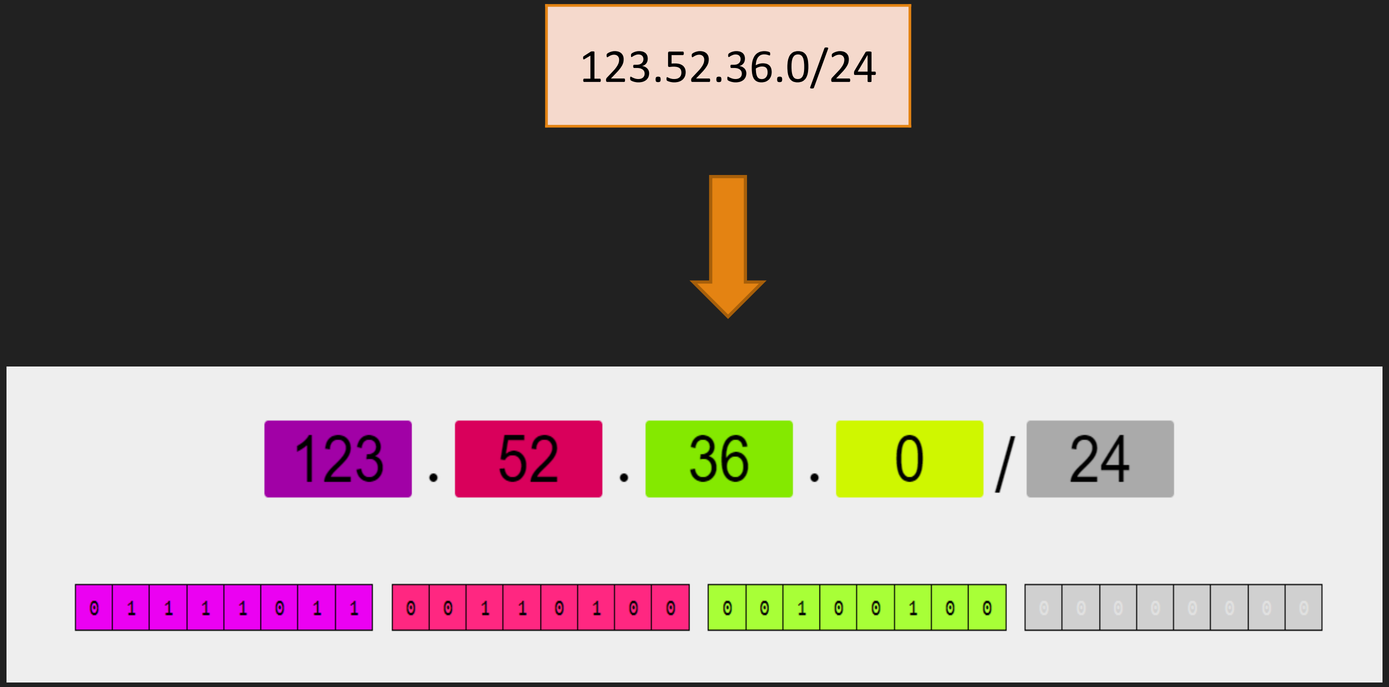
Classless Inter-Domain Routing

123.52.36.0
123.52.36.1
123.52.36.2
123.52.36.3
123.52.36.4
123.52.36.5
123.52.36.6
123.52.36.7
123.52.36.8
123.52.36.9
123.52.36.10
123.52.36.11

123.52.36.0 / 24

123.52.36.0/24

CIDR notation



123.52.36.0

123.52.36.1

123.52.36.2

123.52.36.3

123.52.36.4

||

||

||

||

||

123.52.36.254

123.52.36.255

CIDR Notation

123.52.36.0/28	28 bits are fixed	4 bits are variable	Total IP address – 2^4 = 16
123.52.36.0/31	31 bits are fixed	1 bit is variable	Total IP address – 2^1 = 2
0.0.0.0/32	32 bits are fixed	0 bits are variable	Total IP address – 2^0 = 1
0.0.0.0/0	0 bits are fixed	32 bits are variable	Total IP address – 2^{32} = 4,294,967,296

RFC 1918

Standard for Private IP addressing

Class	Internal Address Range	CIDR Prefix
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

VPC & Subnets

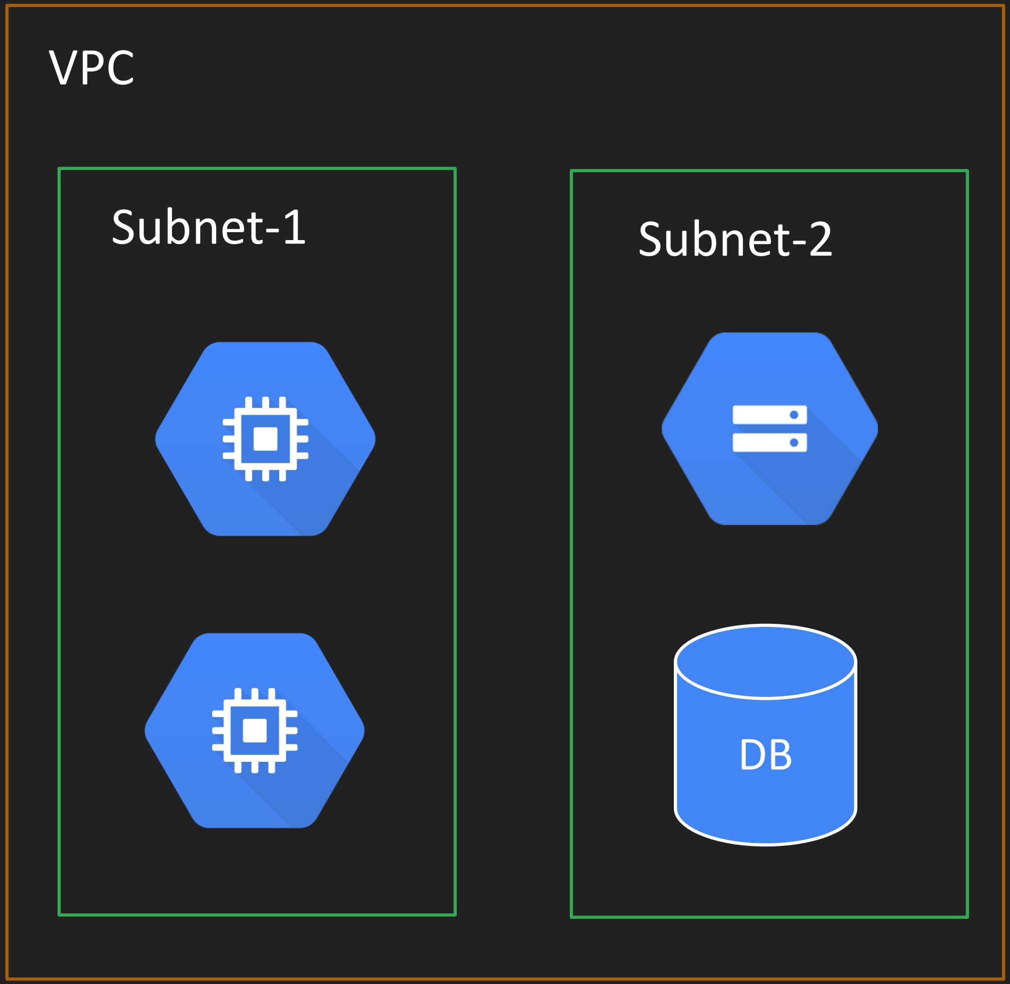
BY ANKIT MISTRY

VPC – Subnetworks

- No Network -> No Cloud
- Virtual version of a physical network
- Networks are part of projects
- It’s Global resources
  - Does not belong to any Region
- Placeholder to keep your resources
- Max 5 VPC per project
- No IP Assigned to VPC

- Network contain subnets
- Subnets are used for segregate resources
- Subnets has IP ranges
  - Expressed as CIDR notation
- VPC must have minimum one subnet
- Subnet belongs to one single region in GCP

VPC - Subnetworks



Default VPC

BY ANKIT MISTRY

Skip Default Network Creation Org Policy

BY ANKIT MISTRY

Create VM with Default VPC

BY ANKIT MISTRY

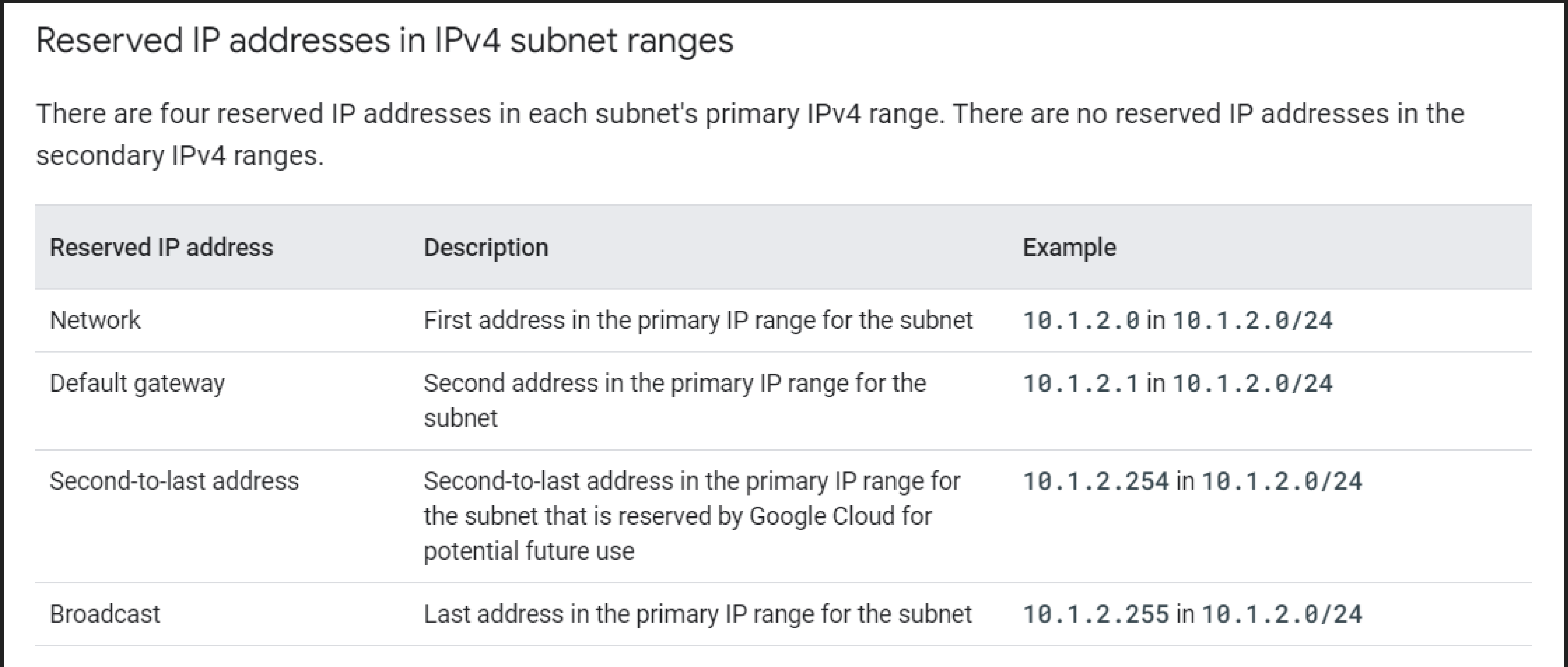
Avoid Default VPC

BY ANKIT MISTRY

Avoid Default VPC

- Lots of unnecessary subnets
- Same name – confusion
- Broad ranges in IP address
- Can not delete subnet
- Default Firewall rules are broad
- Can not go beyond /16

Reserved IP Address in Subnet



Reserved IP addresses in IPv4 subnet ranges

There are four reserved IP addresses in each subnet's primary IPv4 range. There are no reserved IP addresses in the secondary IPv4 ranges.

Reserved IP address	Description	Example
Network	First address in the primary IP range for the subnet	`10.1.2.0` in `10.1.2.0/24`
Default gateway	Second address in the primary IP range for the subnet	`10.1.2.1` in `10.1.2.0/24`
Second-to-last address	Second-to-last address in the primary IP range for the subnet that is reserved by Google Cloud for potential future use	`10.1.2.254` in `10.1.2.0/24`
Broadcast	Last address in the primary IP range for the subnet	`10.1.2.255` in `10.1.2.0/24`

https://cloud.google.com/vpc/docs/subnets#ipv4-ranges

Types of VPC

Default

- Created when compute engine API enabled
- Every project has default VPC
- There is one subnet per regions

Auto

- With Auto mode, Default VPC can be created
- Fixed subnetwork ranges per region
- Can expand from /20 to /16
- Default firewall can be added easily.

Custom

- No Subnet automatically created
- Subnet creation manual
- Custom IP range allocation
- No necessary to create subnet in each region

Create Default Network - Auto Mode

BY ANKIT MISTRY

Create Custom VPC

BY ANKIT MISTRY

Create VM with Custom VPC

BY ANKIT MISTRY

Add More Subnets

BY ANKIT MISTRY

[Hands-on] Reserved IP Address in Subnet

BY ANKIT MISTRY

VM - to - VM Communication

BY ANKIT MISTRY

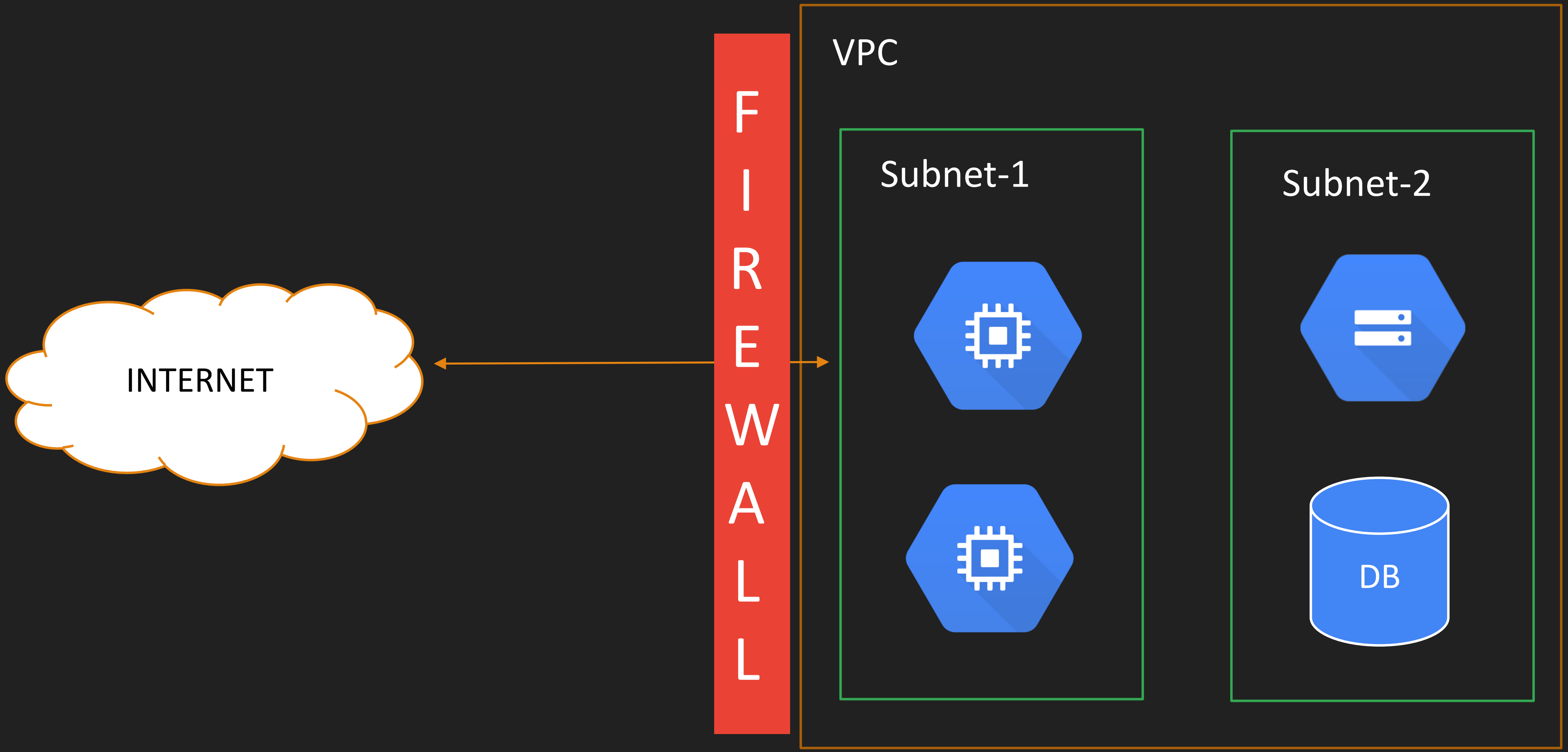
Common Protocol

BY ANKIT MISTRY

SSH, ICMP & http Protocol

- SSH - Secure Shell Protocol – Port 22
  - network communication protocol that enables two computers to communicate
- ICMP – Internet Control Message Protocol - Ping
  - To diagnose network communication issues
- Http – Hypertext transfer Protocol – Port 80
  - Http is used to transfer hypertext such as web pages

Firewall



© ANKIT MISTRY – GOOGLE CLOUD

Firewall rules

- Firewall rules control incoming or outgoing traffic to an instance.
- Trust nothing by default
- Some default rule :
  - Allow all outgoing traffic - egress
  - Deny all incoming traffic - ingress
- Rule has priority number : (0-65535)
  - Lower the number higher priority
- Common port/protocol
  - 22 – SSH, 3389 - RDP
  - ICMP – ping
  - 80 - HTTP/HTTPS

Create First Firewall rule (Allow All Traffic)

BY ANKIT MISTRY

Test Firewall Rule

BY ANKIT MISTRY

VM to VM Communication

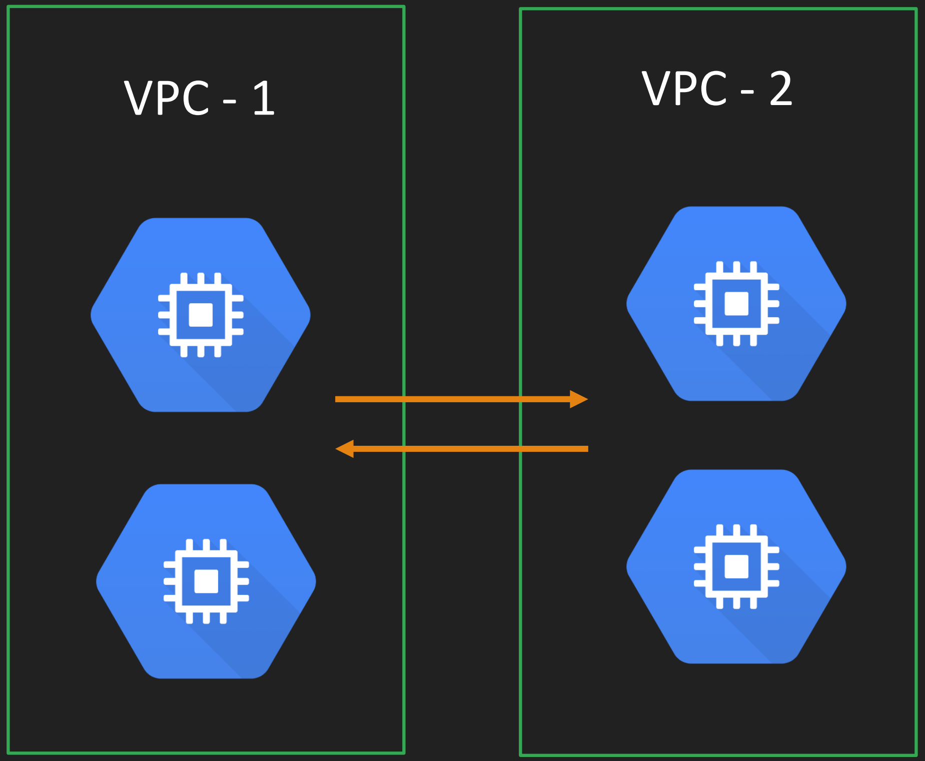
- 2 VM Communication in Same Zone (Same VPC)
- 2 VM Communication in Different Zone of Same Region (Same VPC)
- 2 VM Communication in Different Region (Same VPC)
- 2 VM Communication in Different VPC

VPC network Peering

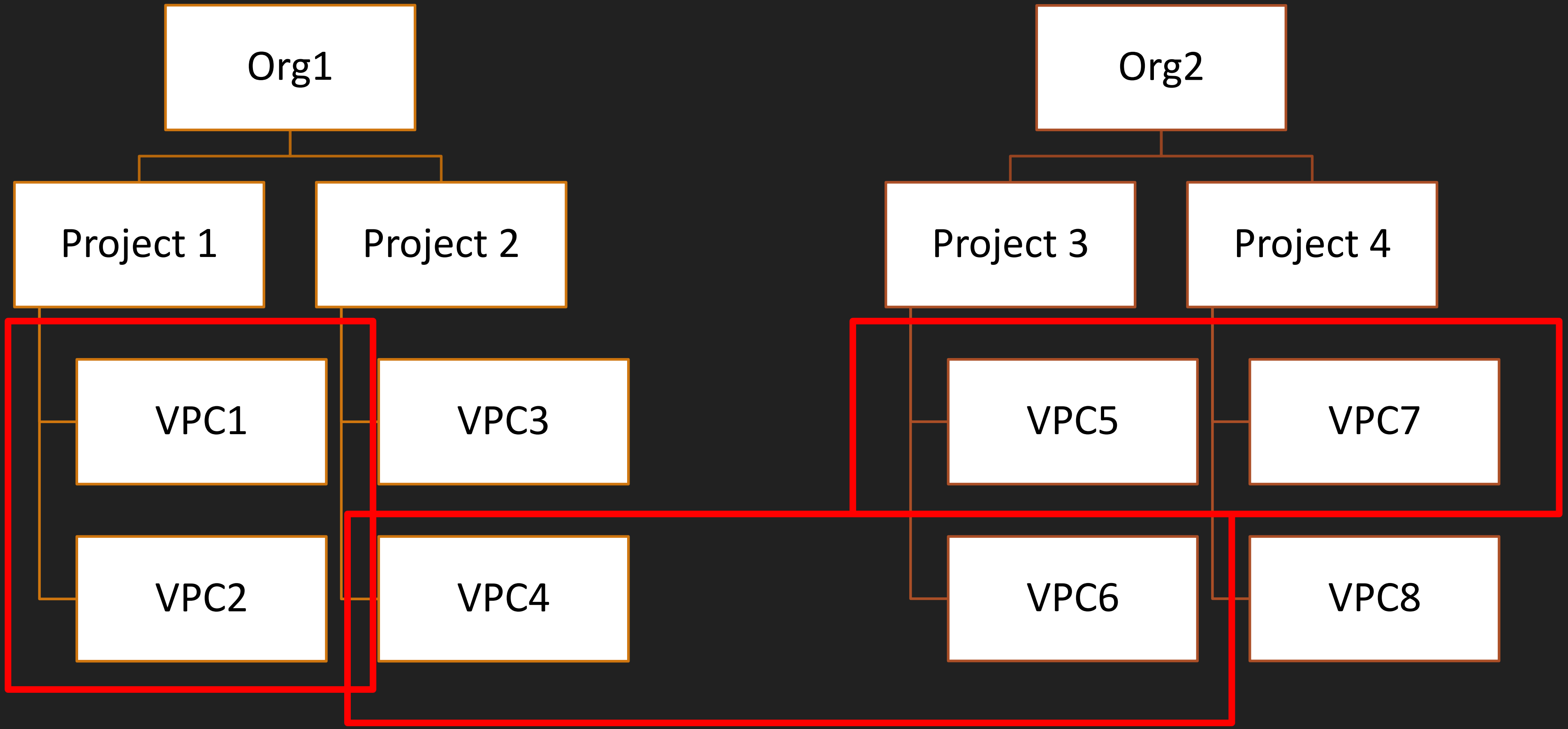
BY ANKIT MISTRY

VPC peering

- No central management
- VPC Managed by individual project team & control all ingress egress traffic
- Use case
  - Project 1 (Ecommerce App) wants to communicate to Project 2 (ML Services App) for Some services like Sentiment Analysis



VPC peering


Org1
Project 1
Project 2
VPC1
VPC2
VPC3
VPC4
Org2
Project 3
Project 4
VPC5
VPC7
VPC6
VPC8

[Hands-on] VPC Network Peering

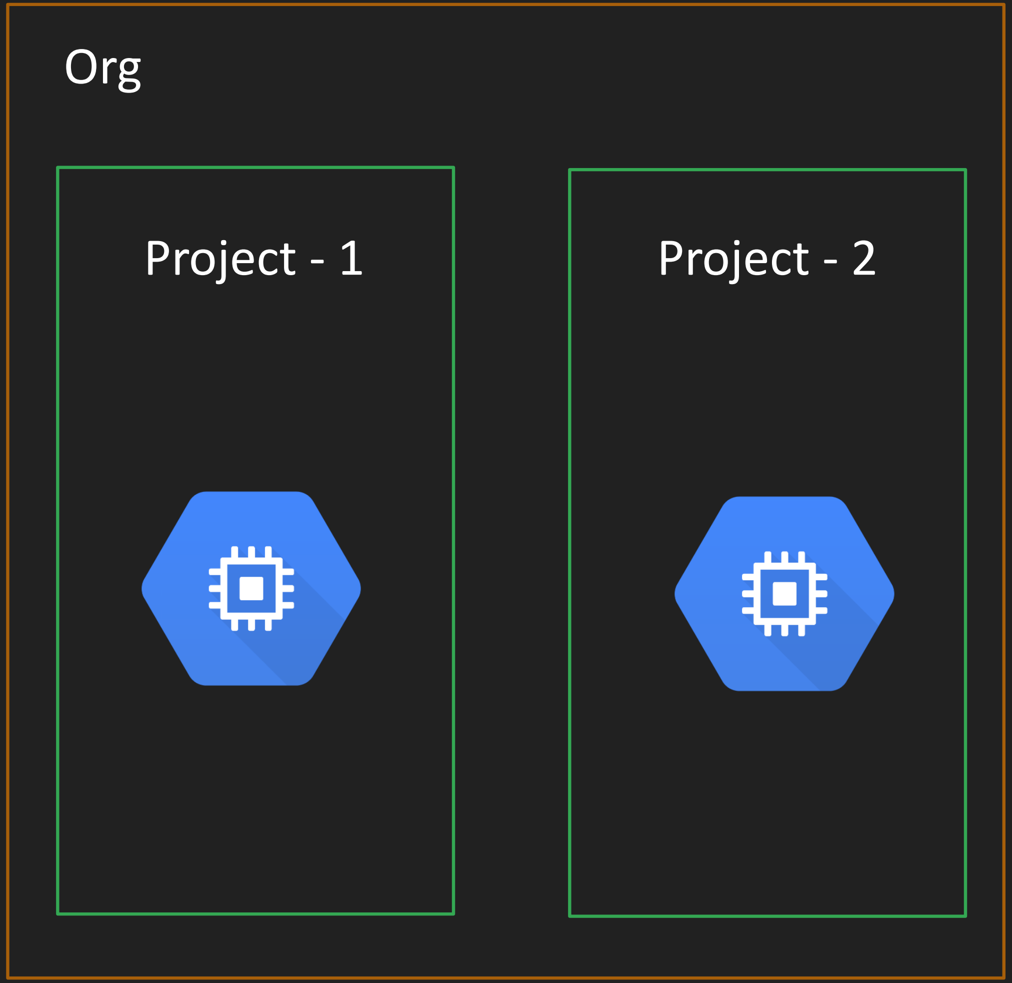
BY ANKIT MISTRY

Centralized VPC

BY ANKIT MISTRY

Shared VPC

- Host Project - Shared VPC
- Multiple Service Project
- Central management of VPC
- Large organization use shared VPC
- Max Host project – 100
- Max Service Project – up to 100
- Shared VPC is only available for projects within an organization node only



[Hands-on]
Shared VPC Demo

BY ANKIT MISTRY

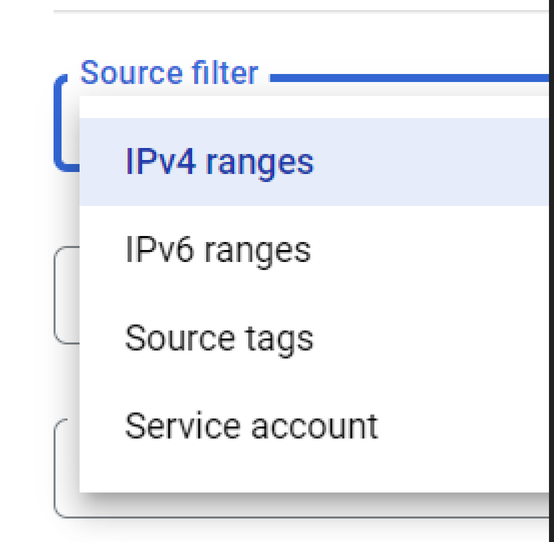
[Hands-on] Shared VPC Demo

- HostProject
  - my-vpc
- ServiceP1
- ServiceP2
- Share my-vpc from HostProject to Service Project

Firewall

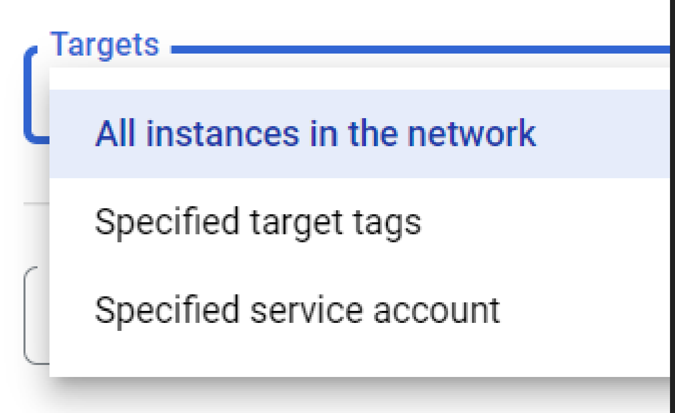
BY ANKIT MISTRY

Firewall Config



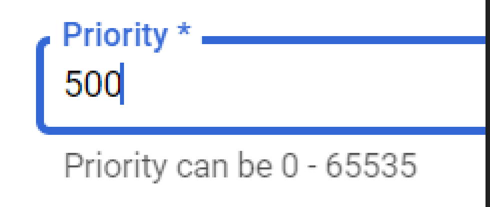
Source filter

- IPv4 ranges
- IPv6 ranges
- Source tags
- Service account



Targets

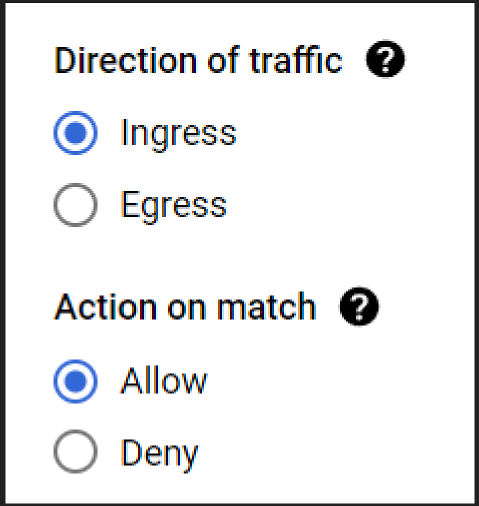
- All instances in the network
- Specified target tags
- Specified service account



Priority *

500

Priority can be 0 - 65535



Direction of traffic ?

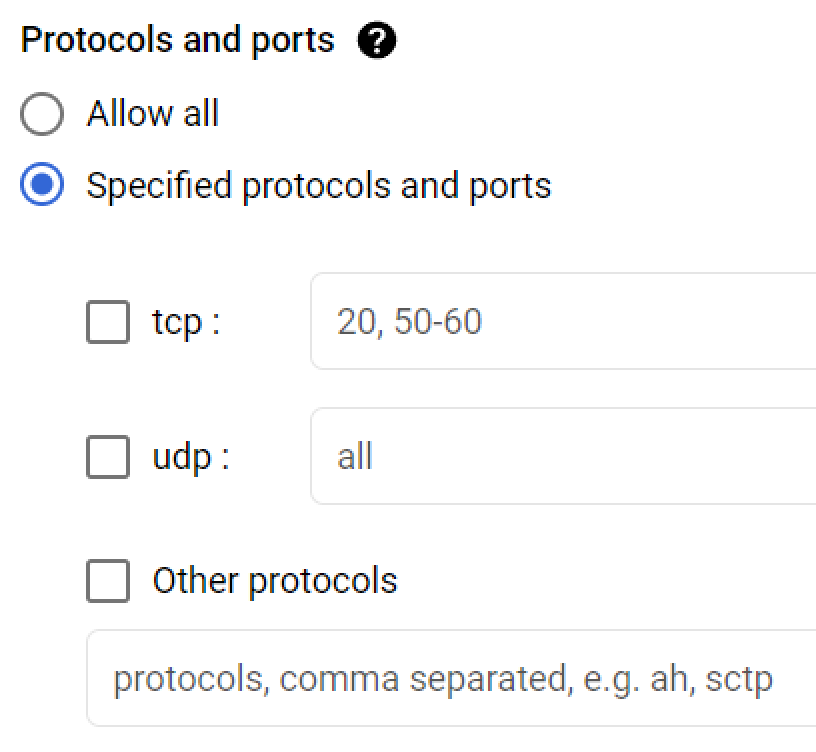
● Ingress

○ Egress

Action on match ?

● Allow

○ Deny



Protocols and ports ?

○ Allow all

● Specified protocols and ports

□ tcp : 20, 50-60

□ udp : all

□ Other protocols

protocols, comma separated, e.g. ah, sctp

Based on IP ranges

- Create 4 VM
- Destination : 2 VM from Above
- Source :
  - Allow Your local machine
  - Allow from Cloud Shell Only
  - Allow whole internet
  - Allow from specific Range in Subnet

Based on Tags

- Allow Specific IP to Target Tags
  - Create 4 VM : vm1, vm2, vm3, vm4
  - Source – Local, Cloud Shell
  - Destination – vm1 tagged, vm2 tagged
- Allow from Source Tags to Specific IP
  - Create Another 4 VM : vm5, vm6, vm7, vm8
  - Source – Tagged from Machine
  - Destination – vm5 (IP), vm6 (IP)

Based on Service Account

- 4 Virtual Machine
- Allow from Specific Service Account to Target IP ALL
  - Source : 2 VM having Specific SA
  - Destination : All machine in Network
    - Allow Your local machine, Cloud Shell Only, whole internet, Specific Range in Subnet
- Allow from Source Tags to Specific SA
  - Source : 2 VM having Tagged
  - Destination : 2 VM having SA

Explore Default Routing Rules

BY ANKIT MISTRY

Expand Subnet Ranges

BY ANKIT MISTRY

Configure Private Access

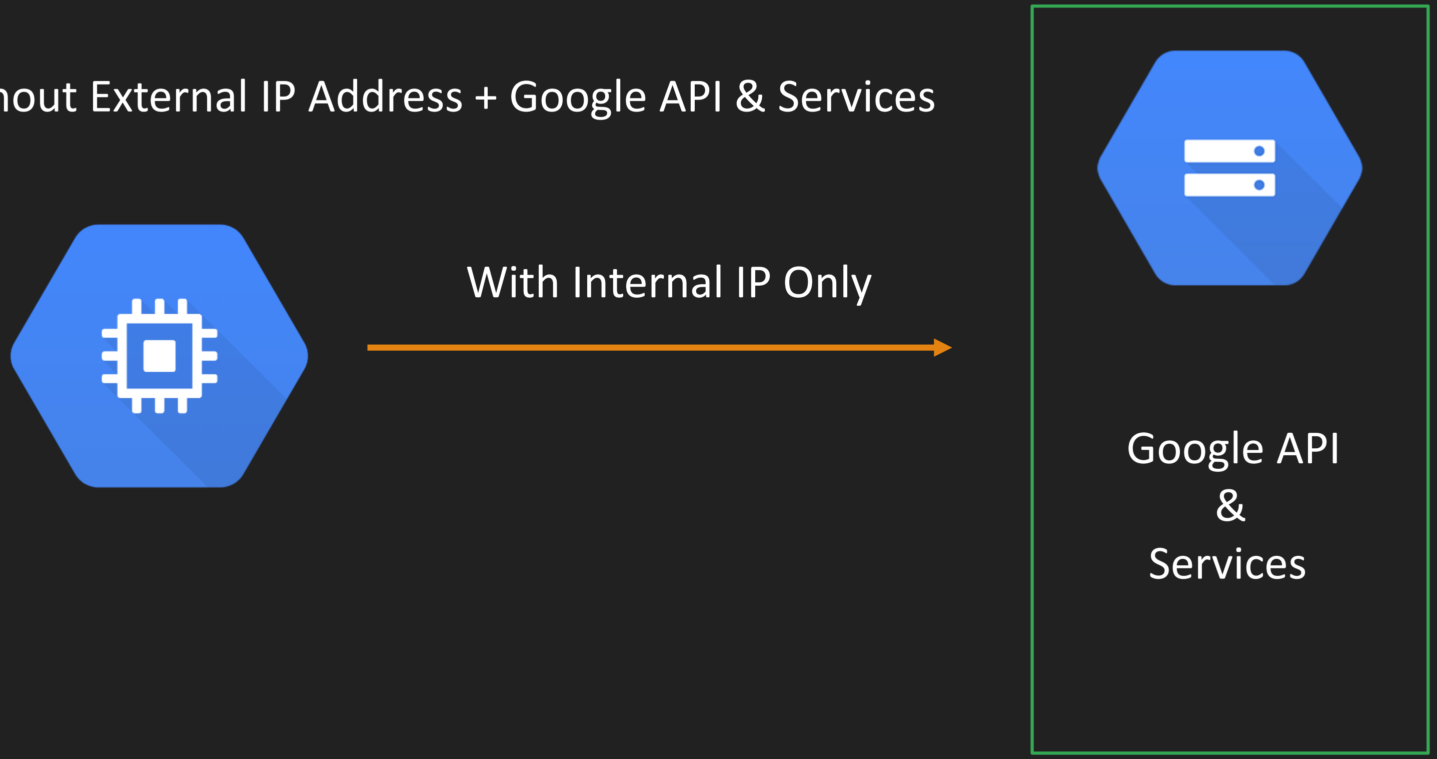
BY ANKIT MISTRY

Private Access

- Private Google Access
- Private Service Access
- Serverless VPC Access

Private Google Access

Access to GCS without External IP Address + Google API & Services

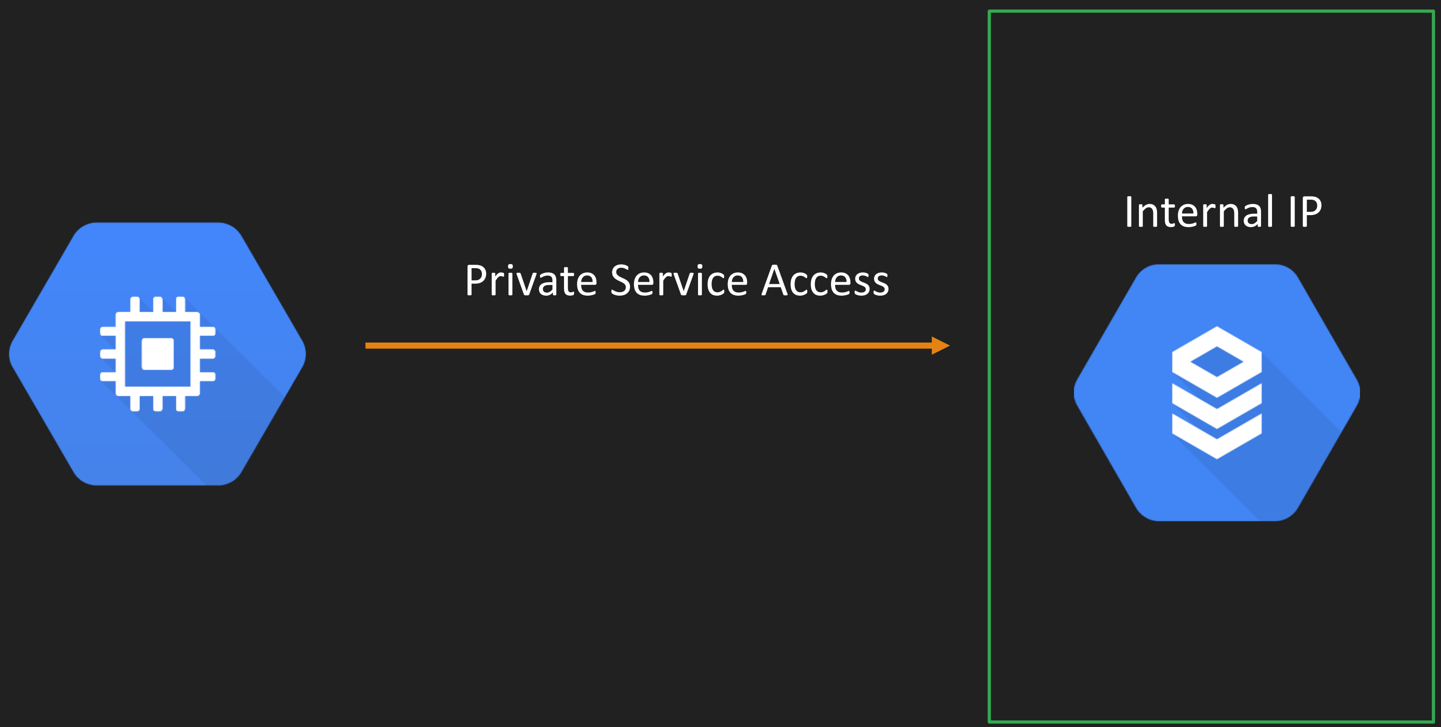


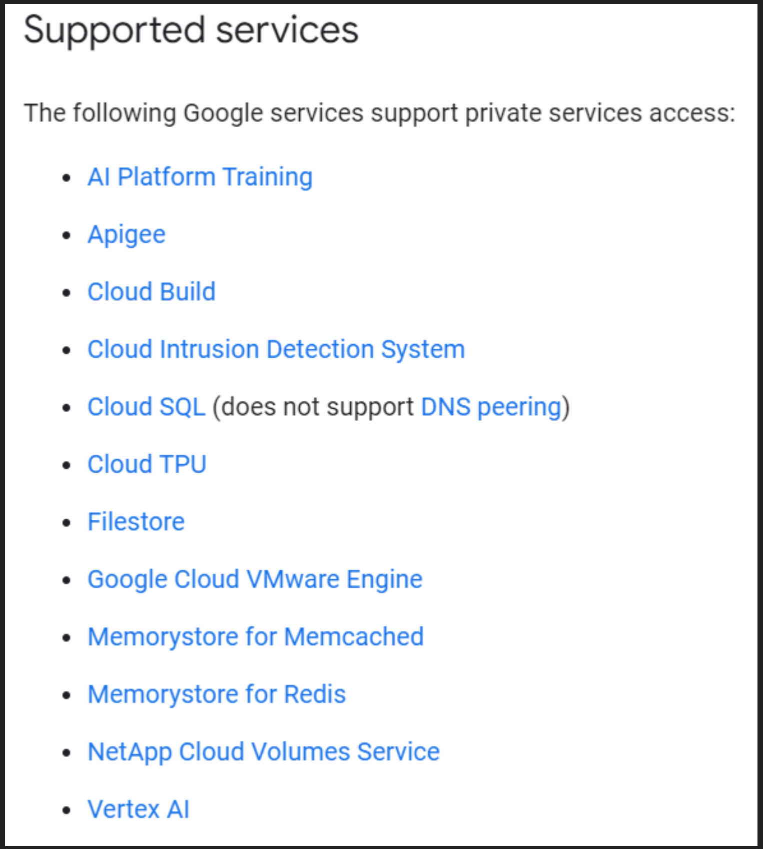
With Internal IP Only

Google API
&
Services

Private Service Access

Access to Cloud SQL, Memory Store with Private IP





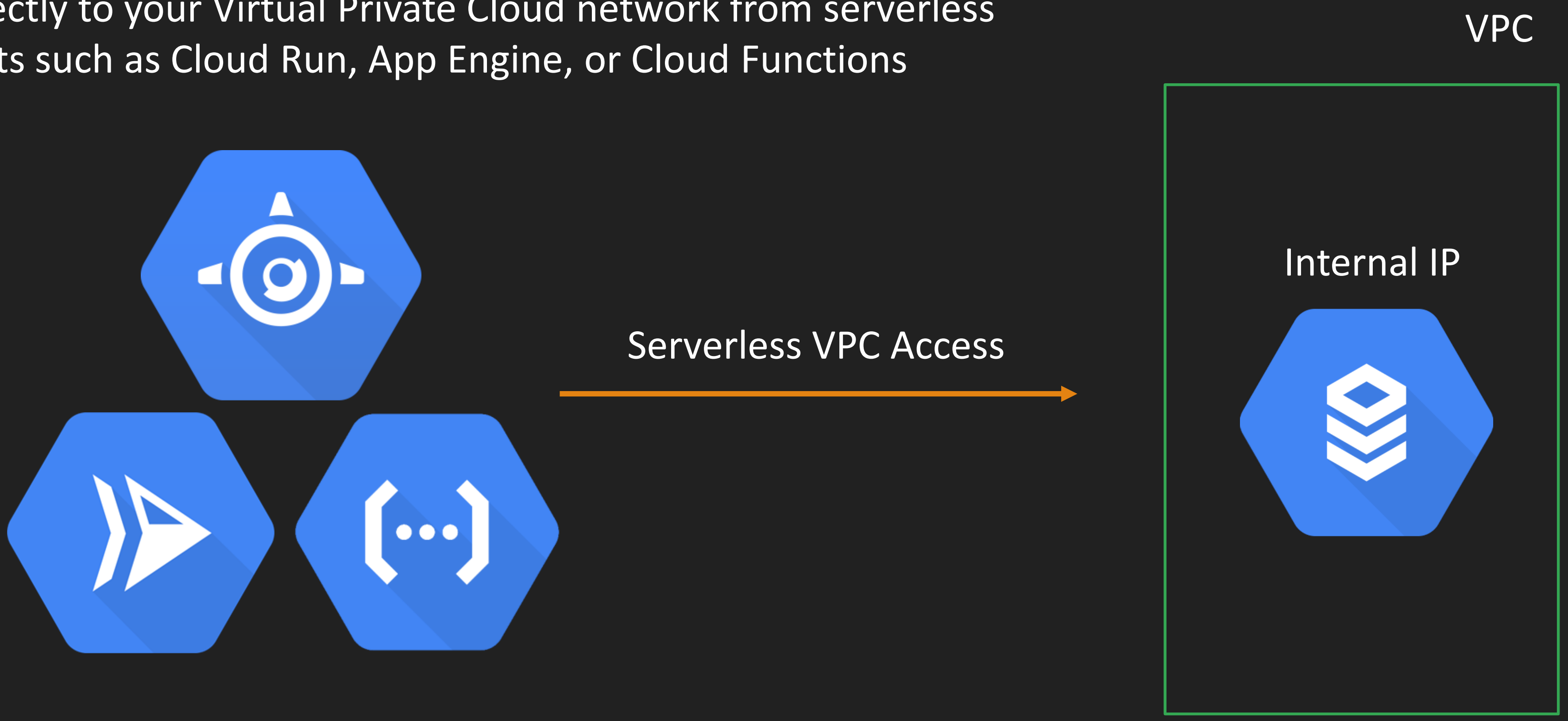
Supported services

The following Google services support private services access:

- AI Platform Training
- Apigee
- Cloud Build
- Cloud Intrusion Detection System
- Cloud SQL (does not support DNS peering)
- Cloud TPU
- Filestore
- Google Cloud VMware Engine
- Memorystore for Memcached
- Memorystore for Redis
- NetApp Cloud Volumes Service
- Vertex AI

Serverless VPC Access

Connect directly to your Virtual Private Cloud network from serverless environments such as Cloud Run, App Engine, or Cloud Functions



Cloud IAP

BY ANKIT MISTRY

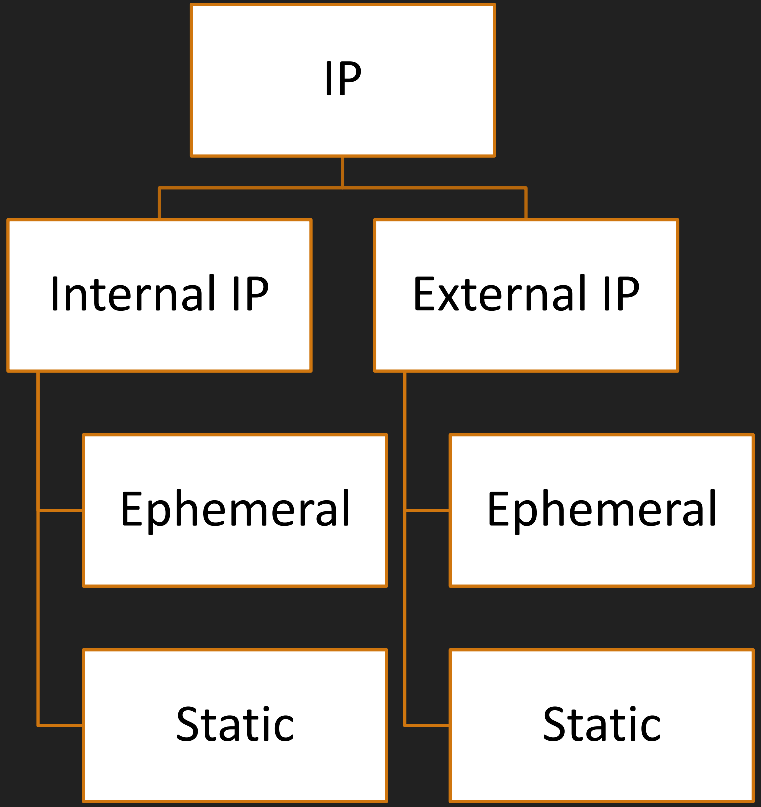
IAP

- Identity aware proxy
- IAP provides a single point of control for managing user access to web applications and cloud resources.
- Manage Http & SSH based resources
- Demo1
  - SSH with just Private IP address
  - Protect Compute Engine SSH Resources, Assign secured tunnel user role
- Demo2
  - Secure Google App engine http resources
  - Assign web app user role
- Demo3
  - Firewall rule - allow SSH to VM(Private IP only) just from browser

Configure IP address

BY ANKIT MISTRY

Types of IP



- Internal IP - Private IP – access from Private Network inside GCP
- External IP – Public IP - Access from anywhere on internet
- Ephemeral IP are temporal, once we restart resource, new IP will be assigned.
- Static – Permeant IP – Can be assigned from one resource to another resources.
- Pricing – will be discussed later
- Reserved IP addresses in IPv4 subnet ranges
  - https://cloud.google.com/vpc/docs/subnets

IP Pricing

- There is no charge for static or ephemeral internal IP addresses.
- For external IP address
  - https://cloud.google.com/vpc/network-pricing

Multiple NIC

- How can you deploy multiple app with different IP on same VM
- Multiple NIC can be attached with Compute Engine
- Each NIC is like One VPC
- Max 8 NIC can be attached
- Disadvantage : overhead to maintain multiple VPC
- Demo

Alias IP & Secondary IP ranges

- Subnet Can have secondary IP apart from Primary ranges
- Ranges of IP address can be attached with Compute engine, Kubernetes as Alias IP
- Not like Multiple VPC, In Single VPC All IP exist
- No need to maintain Multiple VPC
- Demo
  - Create VM with Multiple Range of IPs

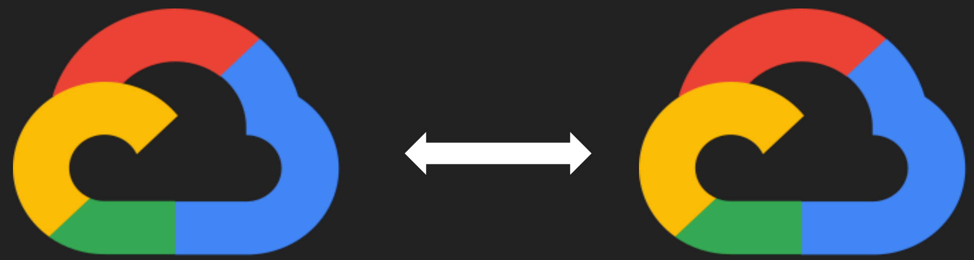
Alias IP in GKE

- Demo
  - Create Public GKE Cluster
  - Private GKE Cluster with Alias IP assignment for Control Plane, Pods, Services

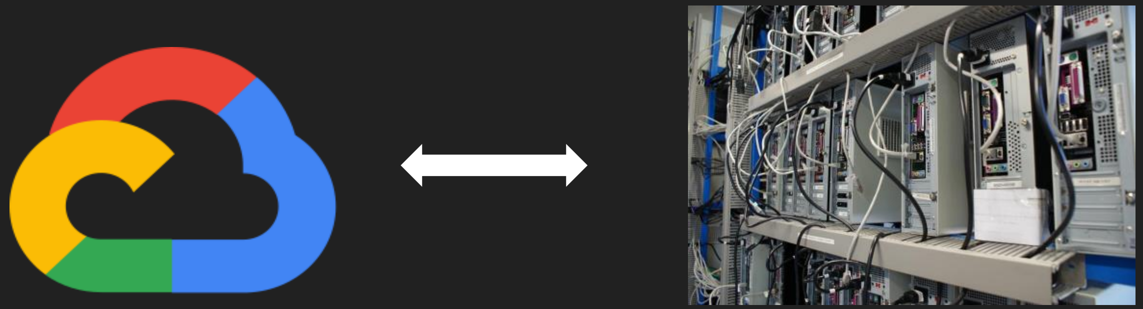
GCP Hybrid Connectivity

BY ANKIT MISTRY

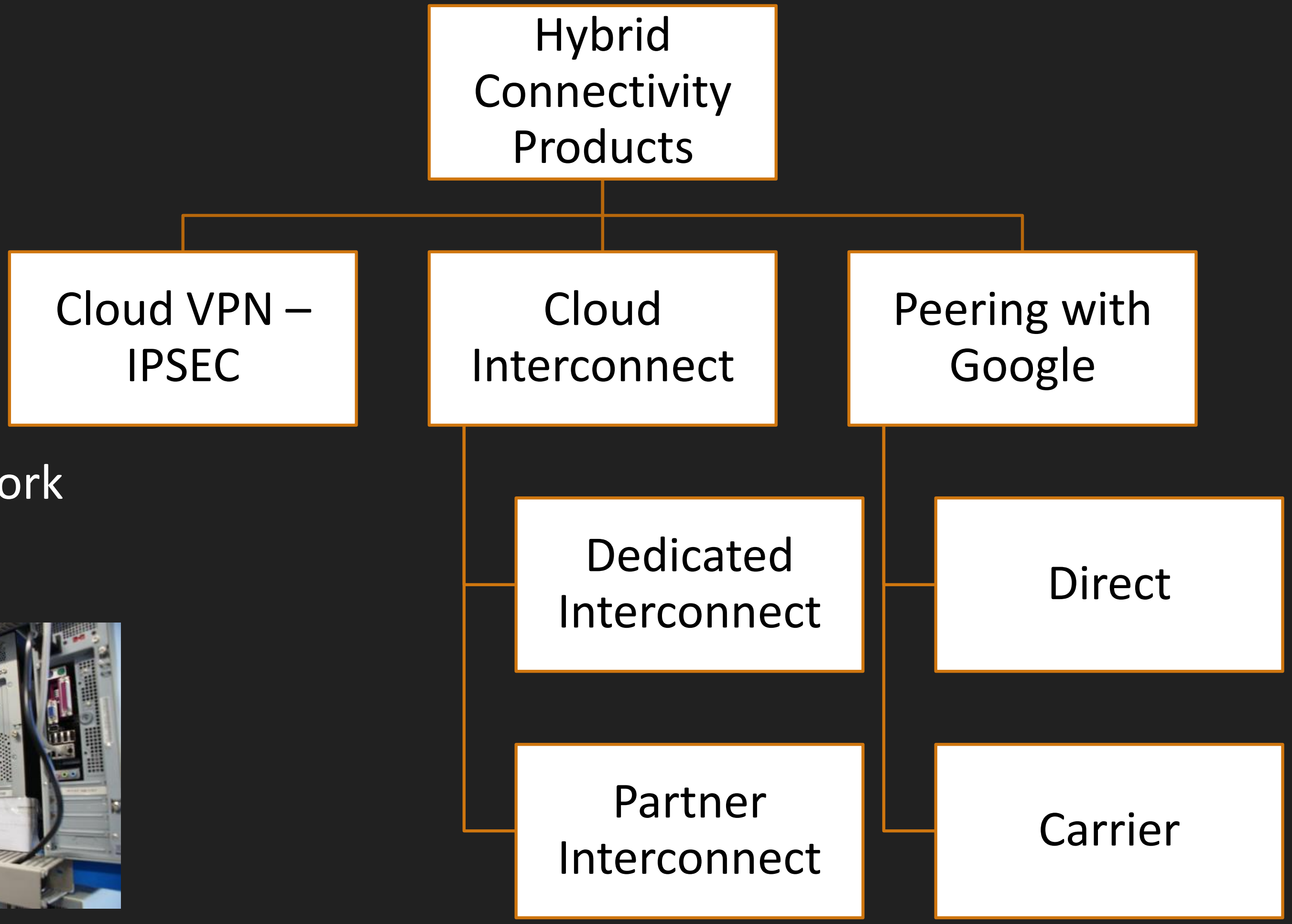
GCP Hybrid Connectivity



Connect your datacenter network with GCP network



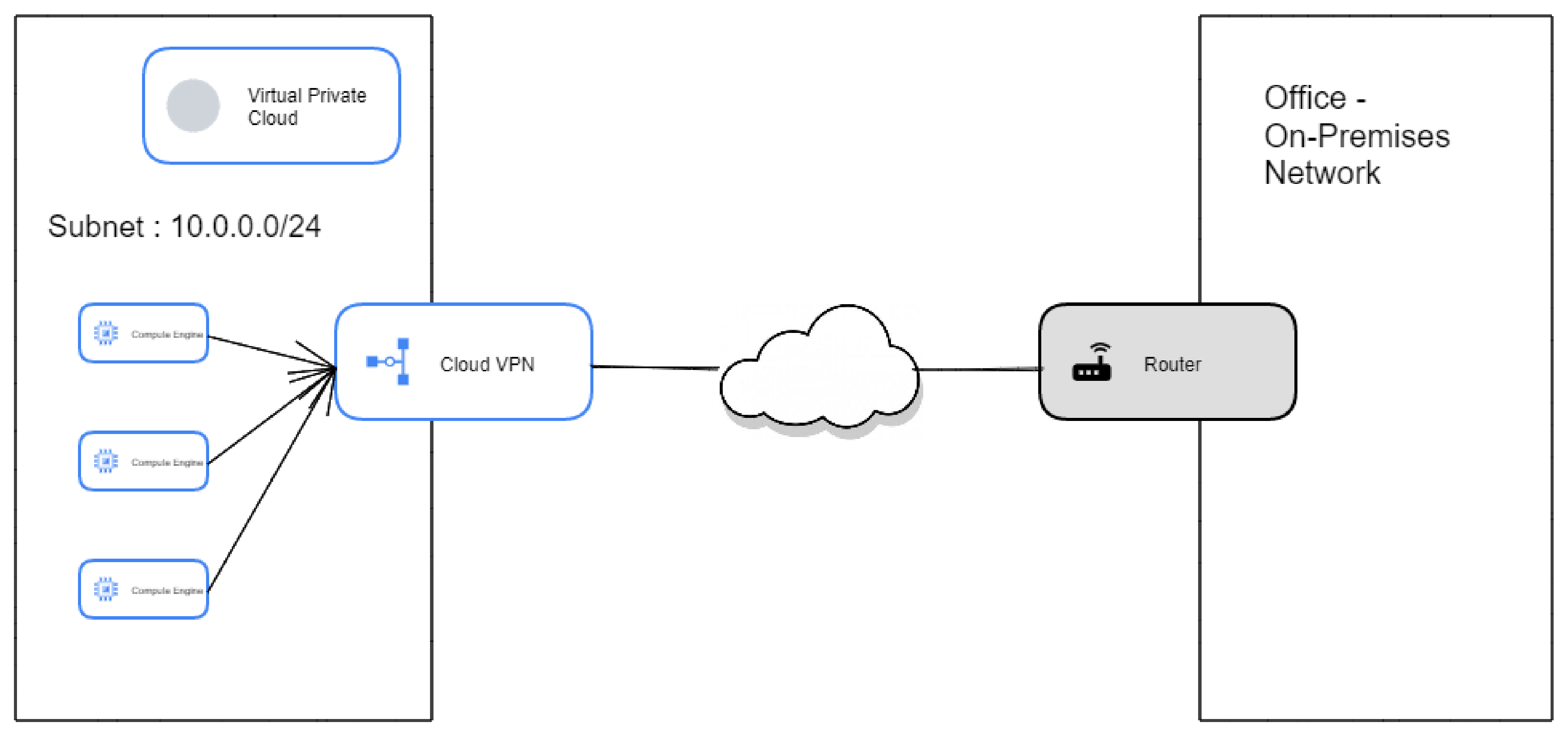
https://pixabay.com/photos/datacenter-bigdata-computer-science-2803200/



Cloud VPN

- A virtual private network lets you securely connect your Google Compute Engine resources to your own private network.
- Cloud VPN securely connects your peer network to your Virtual Private Cloud (VPC) network through an **IPsec VPN**
- It works between
  - Google cloud & datacenter
  - Google cloud & other public cloud (AWS)
- If you want to **quickly** setup connectivity, Cloud VPN is good choice.
- Traffic is **encrypted** by one VPN gateway and then decrypted by the other VPN gateway.
- Traffic travelled over **public** internet
- Single Cloud VPN tunnel can support up to **3 Gbps** bandwidth
- VPC Peering is not transitive in nature. Cloud VPN is transitive.

Cloud VPN


Virtual Private Cloud
Subnet : 10.0.0.0/24
Compute Engine
Compute Engine
Compute Engine
Cloud VPN
Router
Office - On-Premises Network

Cloud VPN Demo

- Total 3 Demo
- Follow all 3 demo in sequence
- Demo – 1
  - GCP to On-premise Setup is difficult
  - GCP to GCP
  - Route based policy

My First Project : Project1

mfp-vpc
============

sub-us : 10.0.0.0/24
allow ssh, icmp
static-us
vm-us
tunnel + gateway creation

GCP Network : Project2

gcp-nw-vpc
================

sub-sg : 192.168.0.0/24
allow ssh, icmp
vm-sg
static-sg
tunnel + gateway creation

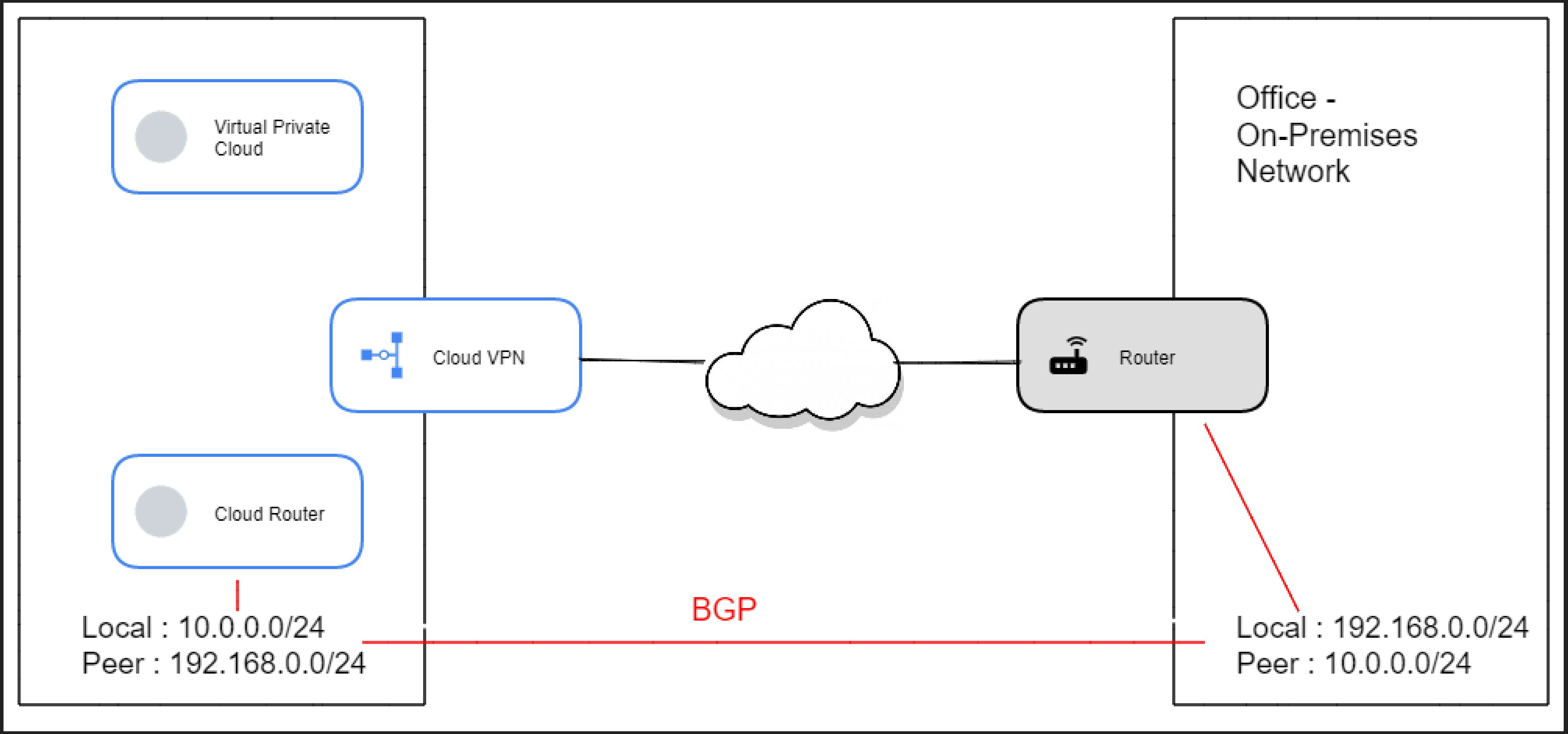
Cloud VPN Demo

- Demo – 2 (Static routing)
  - Add New Subnet
  - Create New VM & Test Connectivity with Old VM
  - Manual Route
- Demo – 3 (Dynamic Routing)
  - Dynamic Routing – based on BGP
  - Create Cloud Router on both side
  - Create another subnet in same region and check advertisement done or not.
- Demo – 4
  - Create subnet in other region and check advertisement done or not.

Cloud Router

- **Cloud Router** is a fully distributed and managed Google Cloud service that uses the Border Gateway Protocol (**BGP**) to advertise IP address ranges
- Router detect all changes and create new optimal routes – like Google Maps
- It makes intelligent decision and exchange information in network
- Discovery of remote networks
- Ability to find a new best path if the current path is no longer available

Cloud Router



Static vs Dynamic Routing

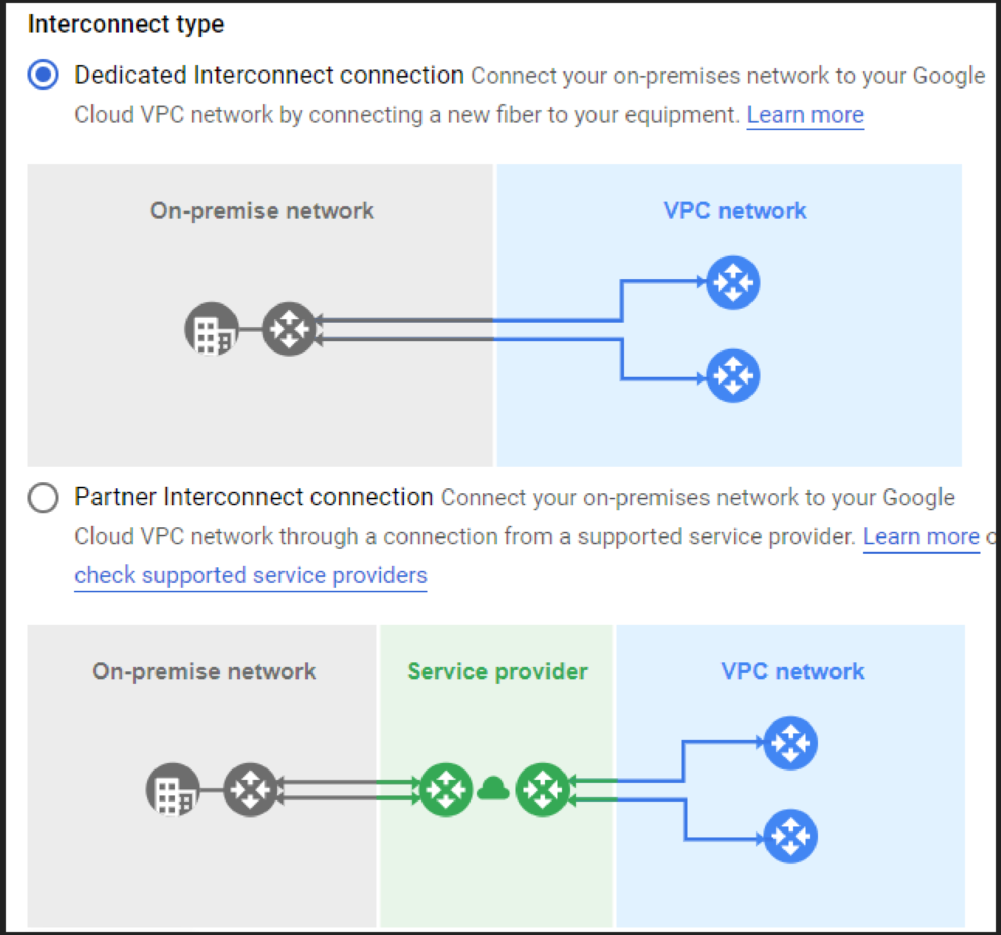
Static Routing	Dynamic Routing
Manual update require	Update routes based on BGP (border gateway protocol)
Downtime – when tunnel deleted	No Downtime
No Standardization	BGP
Static routes are great for stable networks that don’t change	Dynamic routes updates automatically

Cloud NAT

- NAT – network address translation
- How can you (sudo apt update) with just internal IP address from GKE Private Cluster
- How to access
  - GCS services
  - Cloud SQL, Vertex AI, memory store
  - sudo apt update
  - Reach anywhere on internet
- Cloud NAT is the solution which allows VM to connect internet without External IP
- Cloud NAT is bind to VPC – Region.
- Hands-on Cloud NAT Demo

Cloud Interconnect

- ➢ Extend your on premises VPC to GCP network
- ➢ highly available, low latency connection
  - ➢ Cloud VPN use Public internet.
- ➢ Access resource with Internal IP address only
- ➢ Require time for initial setup
- ➢ Once setup, it works with very low latency & with Internal IP address
- ➢ No encryption while traffic travelled



Interconnect type

● Dedicated Interconnect connection Connect your on-premises network to your Google Cloud VPC network by connecting a new fiber to your equipment. Learn more

○ Partner Interconnect connection Connect your on-premises network to your Google Cloud VPC network through a connection from a supported service provider. Learn more o
check supported service providers

Create Cloud Interconnect Request

BY ANKIT MISTRY

Dedicated vs partner Cloud Interconnect

Dedicated Interconnect	Partner Interconnect
No Encryption	No Encryption
SLA : Your Datacenter & Google VPC	SLA : Your Datacenter & Google VPC
Pricing is high	Pricing is lower than dedicated
Bandwidth : 10 Gbps to 200 Gbps	Bandwidth : 50 Mbps to 10 Gbps
No Service Provider require	Service Provider require
Internal IP communication	Internal IP communication

Cloud Peering

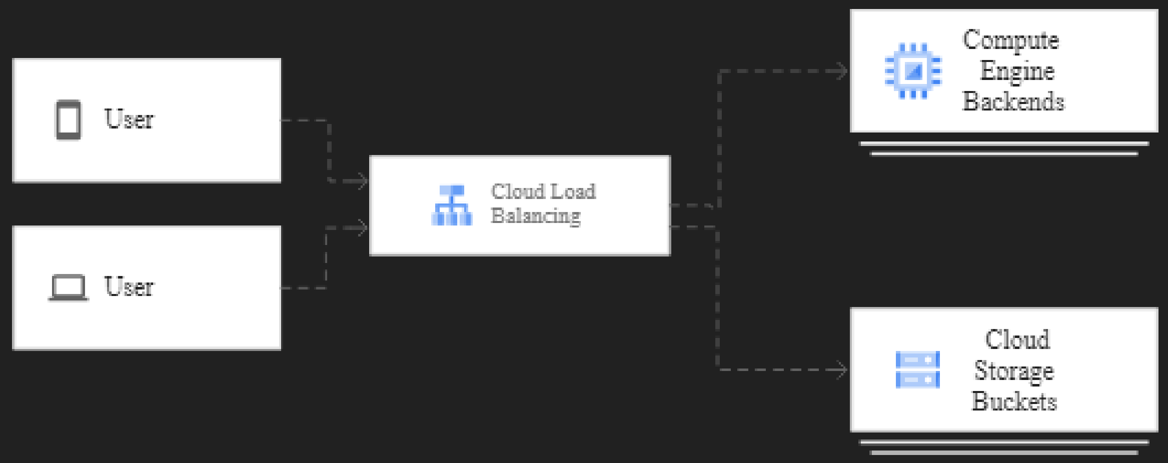
BY ANKIT MISTRY

Cloud Load balancer

BY ANKIT MISTRY

Load balancer

- A load balancer distributes user traffic across multiple instances of your applications.
- By spreading the load, load balancing reduces the risk that your applications experience performance issues



Cloud Load balancer

- Cloud Load Balancing is a fully distributed
- Software-defined managed GCP service.
- It isn't hardware-based, so you don't need to manage a physical load balancing infrastructure.
- Health check
  - route traffic to only healthy instance
  - maintain minimum number of instances
- Auto scaling based on traffic
- High availability
- Single anycast IP

Global vs Regional Load balancer

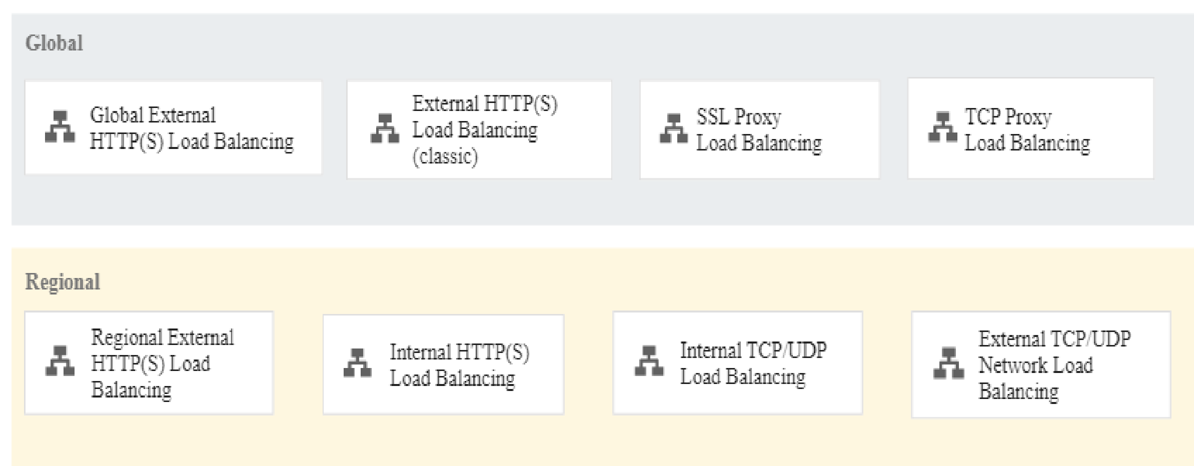
- Use global load balancing when your backends are distributed across multiple regions.
  - You can provide access by using a single anycast IP address.
- Use regional load balancing when your backends are in one region, and you only require IPv4.

Internal vs External LB

- External load balancers distribute traffic coming from the internet to your Google Cloud Virtual Private Cloud (VPC) network. Global load balancing requires that you use the Premium Tier of Network Service Tiers. For regional load balancing, you can use Standard Tier.

- Internal load balancers distribute traffic to instances inside of Google Cloud.

Types of Load balancer



Global

- Global External HTTP(S) Load Balancing
- External HTTP(S) Load Balancing (classic)
- SSL Proxy Load Balancing
- TCP Proxy Load Balancing

Regional

- Regional External HTTP(S) Load Balancing
- Internal HTTP(S) Load Balancing
- Internal TCP/UDP Load Balancing
- External TCP/UDP Network Load Balancing

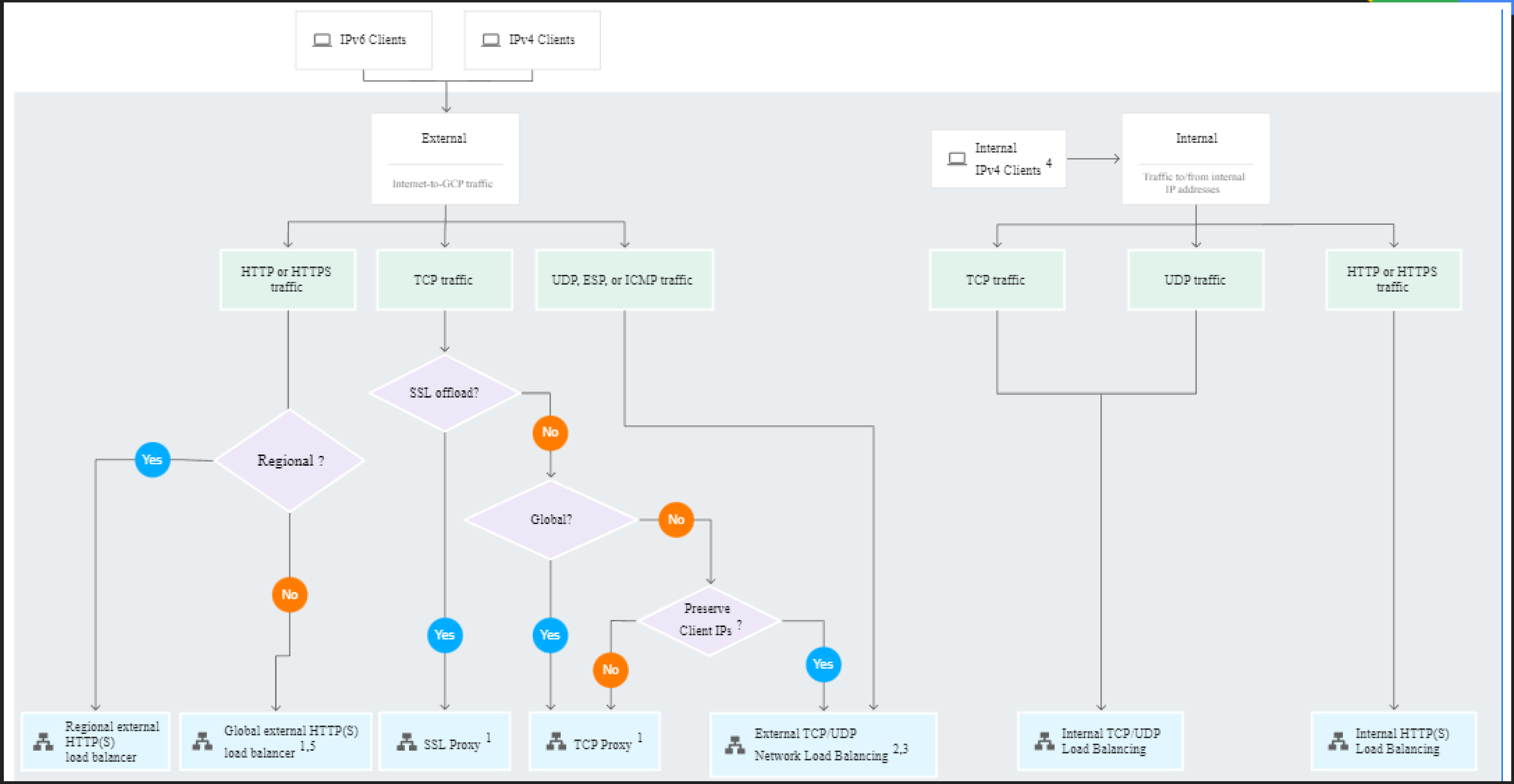
https://cloud.google.com/load-balancing/docs/load-balancing-overview#tech-load-balancing

Layer 4 vs Layer 7 LB

- Layer 4 – TCP/UDP load balancer
  - Distributes traffic based on IP and Port
  - Not much intelligent
  - TCP – Transmission control protocol
    - Reliability is high
  - UDP – User datagram Protocol
    - Performance is good
- Layer 7 – Http/https load balancer
  - Use Data in a packet to distribute traffic
  - Smarter load balancer
  - Most application communicate at layer 7

Layer 7 (Http/Https/SMTP)
Layer 6 – Presentation Layer
Layer 5 – session Layer
Layer 4 (Transport – TCP/UDP)
Layer 3 (network Layer - IP)
Layer 2 – Datalink Layer
Layer 1 – Physical Layer

Choosing Load balancer



[Hands-on]
Cloud Load Balancer

- http/https based load balancing
- 4 Host and path rules
  - hostname/* → Cloud run
  - Cloud DNS Setup
  - hostname/dynamic1/* → Instance Group (MIG)
  - hostname/dynamic2/* → Instance Group (UMIG)
  - hostname/static-images/* → GCS Bucket - images
- Front ends
  - Http
  - Https (With Certificate)

Cloud DNS

BY ANKIT MISTRY

Cloud DNS

- DNS – Address book for internet
- www.google.com --------- 74.125.29.101
- Highly Scalable, Reliable and Managed Domain Name System (DNS) service on GCP infrastructure
- 100% SLA
- Manage millions of DNS zones and records
- Cloud DNS
  - Public Zone
  - Private Zone
- [Hands-on] Cloud DNS – setup for Cloud load balancer

Private Cloud DNS

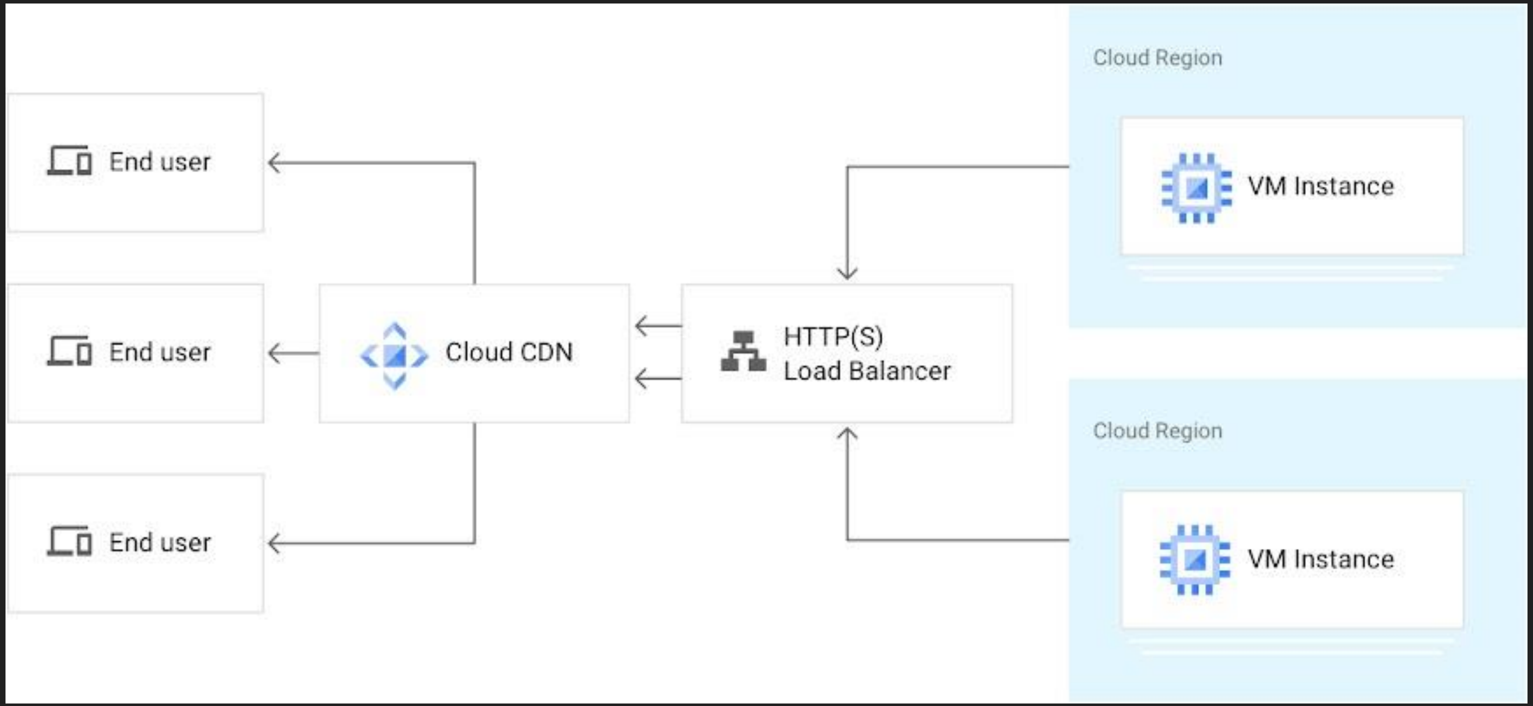
BY ANKIT MISTRY

Cloud CDN

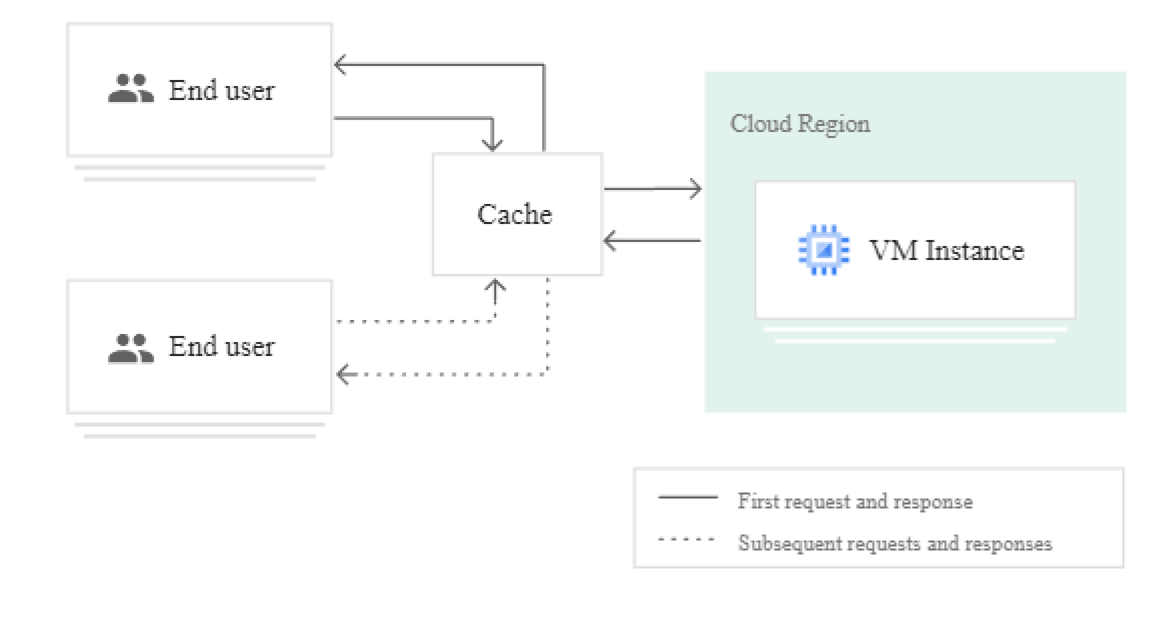
BY ANKIT MISTRY

Cloud CDN

- Content delivery network
- Fast, reliable web and video content delivery with global scale and reach.



Cloud CDN – cache hit miss



Cache hit and cache miss

https://cloud.google.com/cdn/docs/locations

[Hands-on] Cloud CDN

BY ANKIT MISTRY

Cloud Armor

- Network security Product
- Web application firewall (WAF) + DDos attack prevention
- Works for Layer 3 to layer 7
- Intelligent filtering – Not just IP/Port
    - lots of custom rule can be created at L3 – L7
- ML-based Adaptive Filtering
- Works with Cloud Load balancer
- Need to have Org Node
    - can not work with no organization

[Hands-on] Cloud Armor

- Create VM – nginx installed
- Create Unmanaged instance group from VM
- Create Load balancer with Unmanaged IG as backend
- Cloud Armor
  - Create Policy & add rule (attached with load balancer)
  - Rule Default – Deny all
  - Rule 1 : Allow All
  - Rule 2 : Allow from Cloud Shell, not from Local machine
  - Rule 3 : Allow from Local Machine, not from Cloud Shell
  - Create extra path : /goodpath/*, /badpath/*
  - Rule 4 : Create custom expression
    - Allow & Deny based on Path expression

Network Service Tiers

BY ANKIT MISTRY

VPC Flow Logs

BY ANKIT MISTRY

THANK YOU

Google Cloud Certified
PROFESSIONAL
CLOUD NETWORK ENGINEER