Google Cloud Platform – Cloud Architect

Networking

Agenda

- Basics
- Virtual Private Cloud (VPC)
- Bastion Host
- VPC Key Concepts
- Network Service Tier
- Shared VPC
- Shared VPC
- Connect On-Premise/ Other Cloud to GCP
- Typical VPN Setup
- Cloud VPN
- Routes
- Internconnect
- VPN vs Interconnect
- OSI
- Cloud Load Balancer
- Cloud CDN

Basics

Basics – Request for Comment 1918 (RFC 1918)

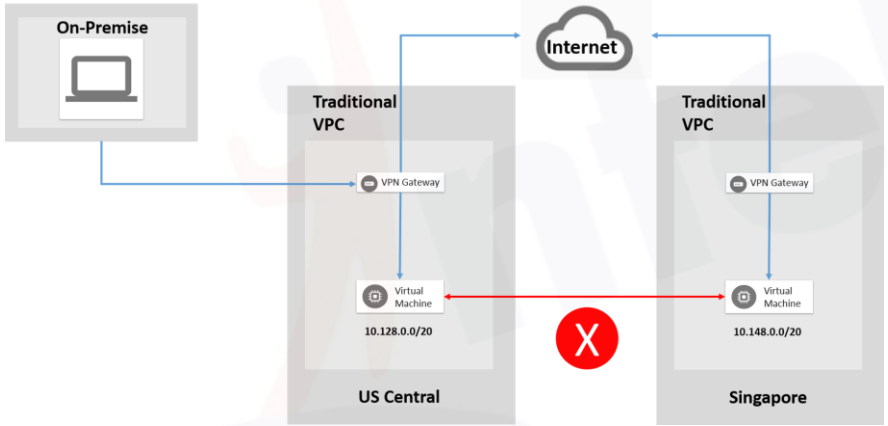
- RFC 1918 was used to create the standards by which networking equipment assigns IP addresses in a private network
- Addresses in one of following ranges are not routed on the Internet backbone. Internet routers immediately discard private addresses

Class/ Block	IP Address Range	CIDR Prefix	No. of Addresses
A/ 24-bit block	10.0.0.0 – 10.255.255.255	**10**.0.0.0/8	16,777,216
B/ 20-bit block	172.16.0.0 – 172.31.255.255	**172.16**.0.0./12	1,048,576
C/ 16-bit block	192.168.0.0 – 192.168.255.255	**192.168**.0.0/ 16	65,536

Virtual Private Cloud (VPC)

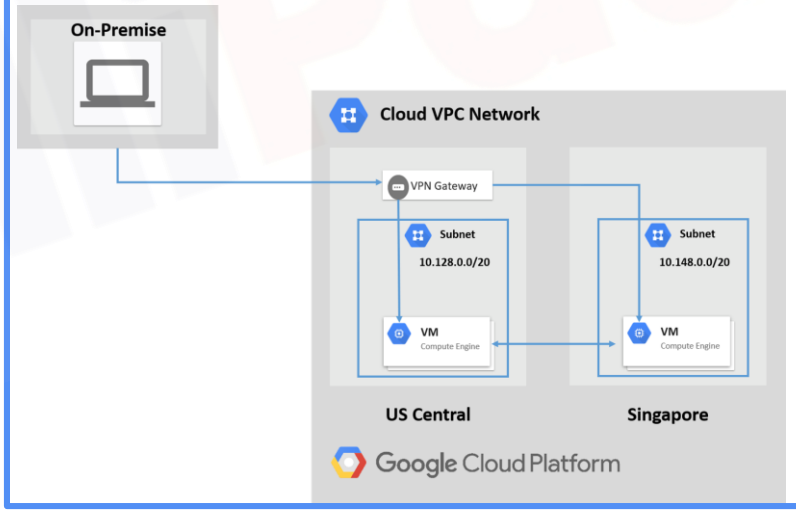
Traditional VPC

- Traditional VPC is regional in nature



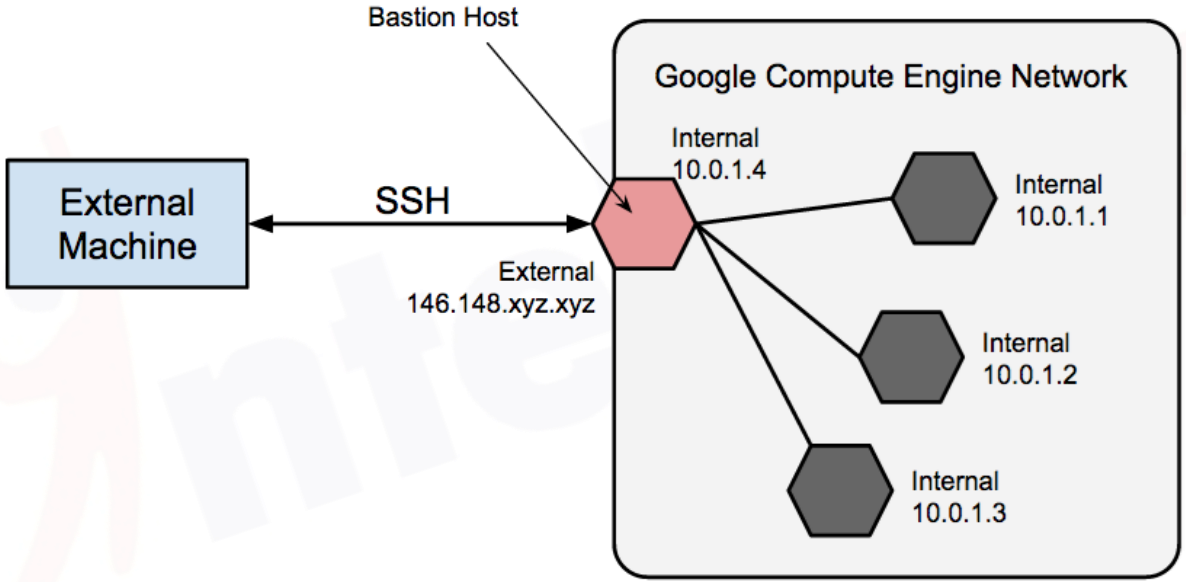
Google VPC

- VPC is global construct



Bastion Host

- Isolates your internal traffic from the external world which avoids Denial of Service (DoS) attack

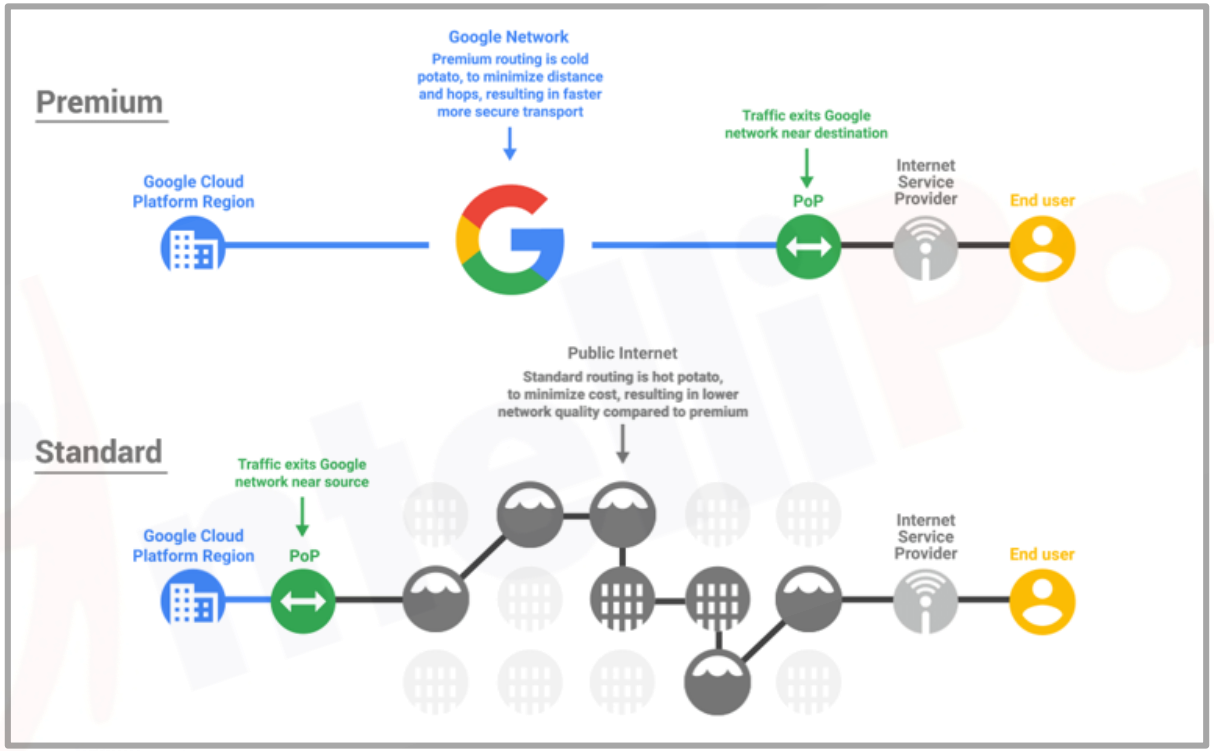


- Source: https://cloud.google.com/solutions/connecting-securely

VPC Key Concepts

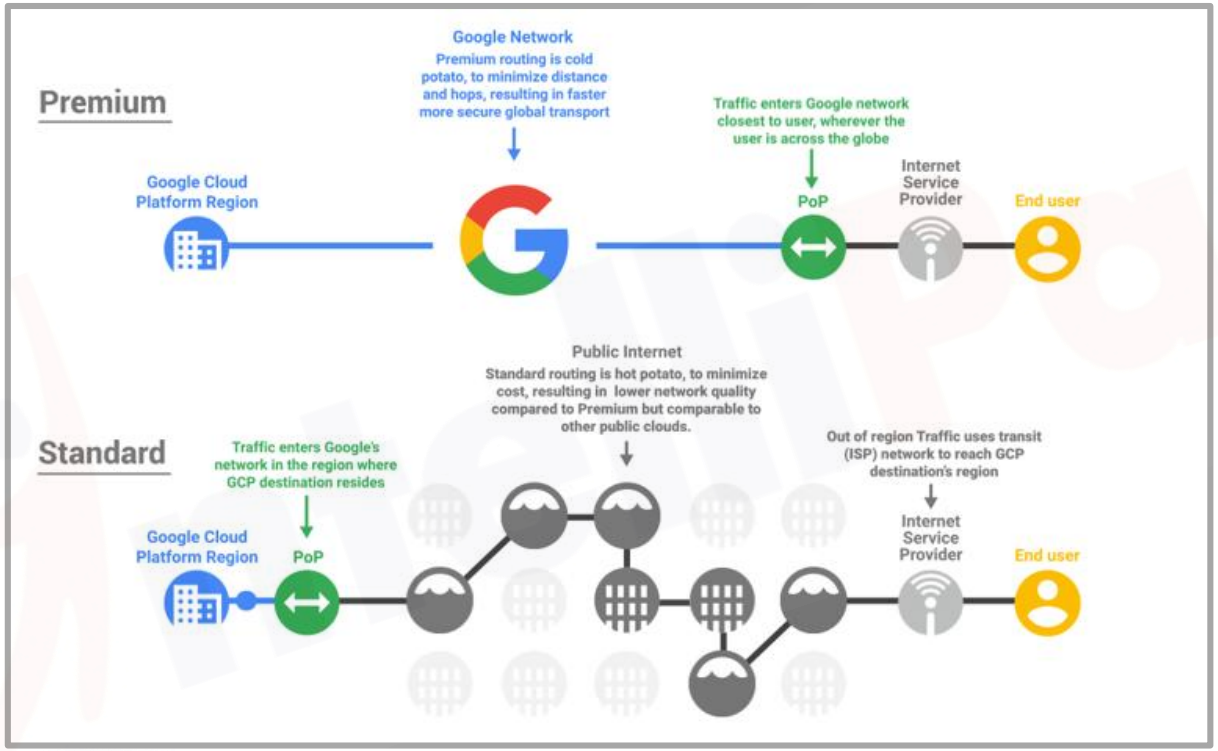
1. VPC networks, including their associated routes and firewall rules are global resources.
2. Subnets are regional resources.
3. Two types of VPC networks available auto and custom based on subnet creation mode.
4. Each project starts with a default auto mode network.
5. Traffic to and from instances can be controlled with network firewall rules.
6. Every new network has two types of system-generated routes.

Network Service Tier



Source: https://cloud.google.com/blog/products/gcp/introducing-network-service-tiers-your-cloud-network-your-way

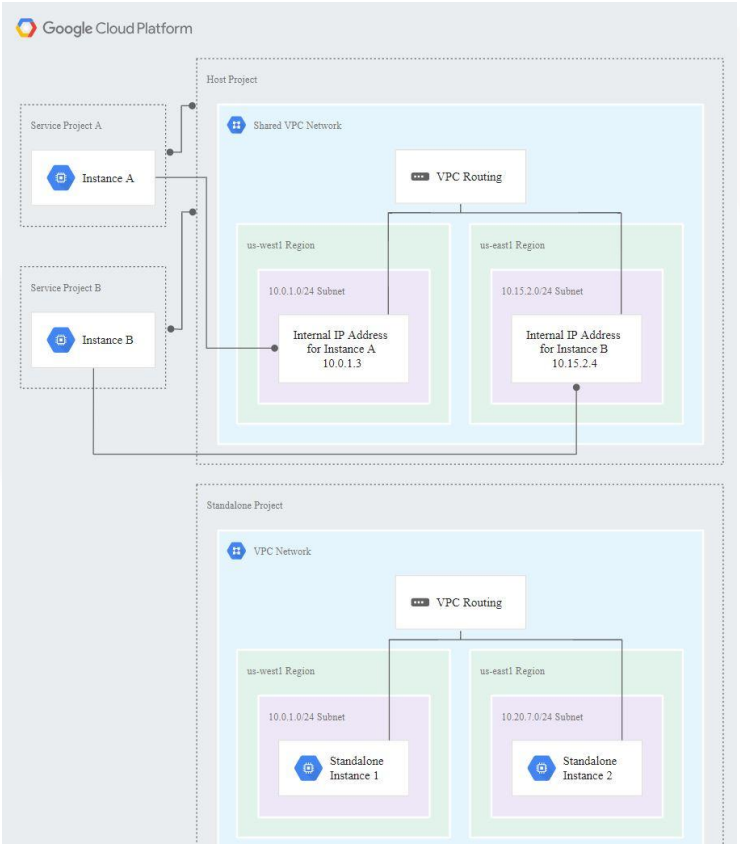
Network Service Tier



Source: https://cloud.google.com/blog/products/gcp/introducing-network-service-tiers-your-cloud-network-your-way

Shared VPC

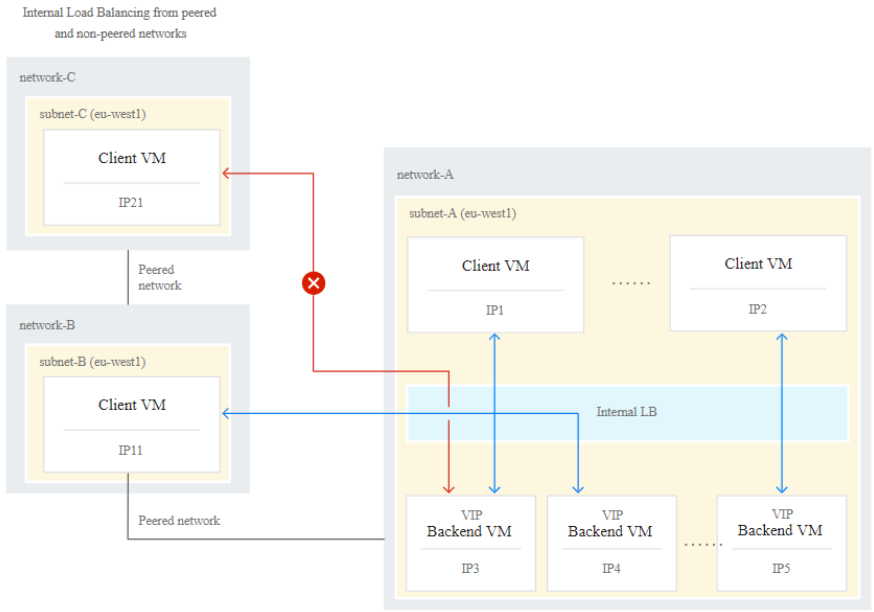
- VPC & Subnetworks can be shared across GCP Projects
- Typically used in large organizations



Source: https://cloud.google.com/vpc/docs/shared-vpc

VPC Peering

- To connect VPC networks with-in/ across Project/ Organization
- Traffic can be travelled across GCP Projects only
- Helps to build SaaS
- 25 peered networks limit



Source: https://cloud.google.com/vpc/docs/vpc-peering

Connect On-Premise/ Other Cloud to GCP

Cloud VPN

- Tested and a reliable way of interconnecting your networks.
- SLAs of 99.9%
- Bandwidth support up to **3Gbps** per tunnel

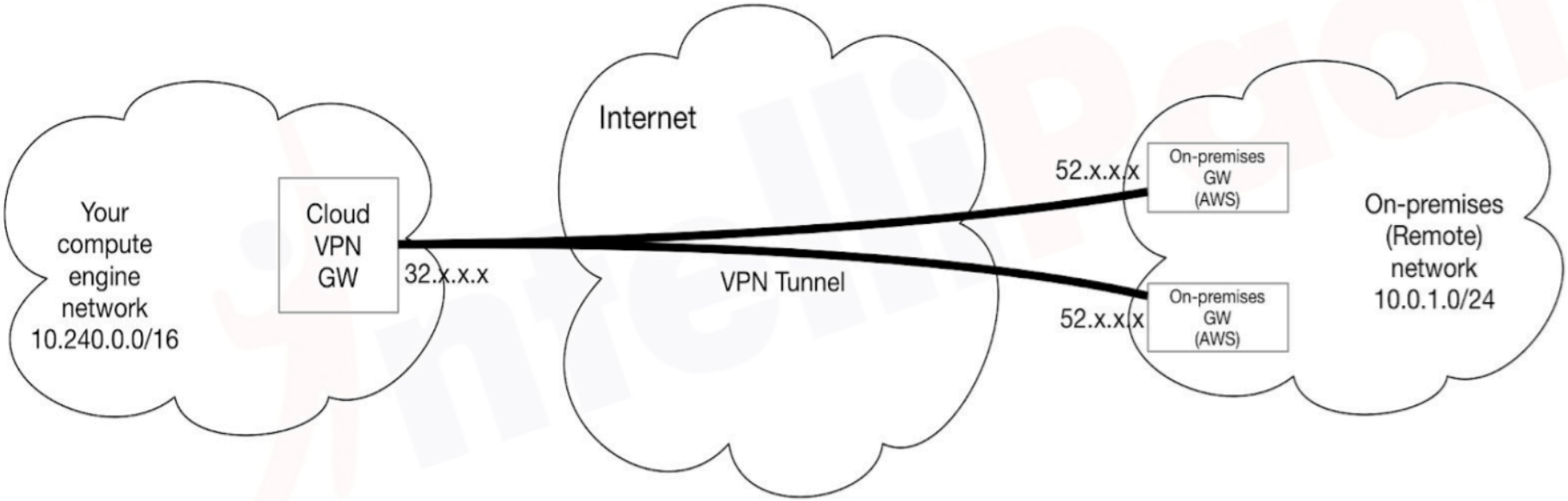
Cloud Interconnect

- Enterprise grade 10G connections or 50Mbps-10G per VLAN via Partner Interconnect
- Industry leading SLAs of 99.99%
- Ultimate Bandwidth

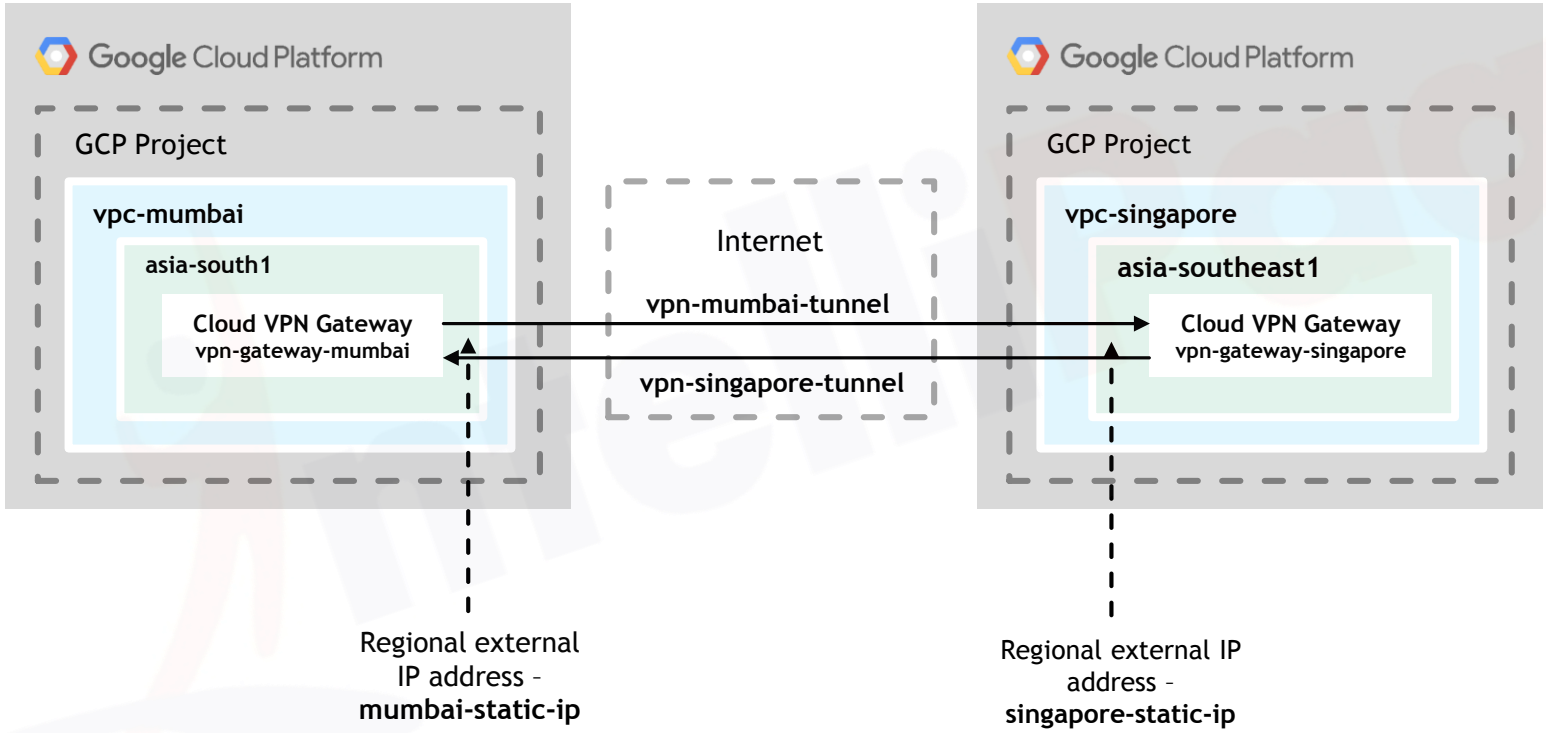
Peering

- If you can meet Google's requirements connect directly using direct peering or pick a partner for partner peering

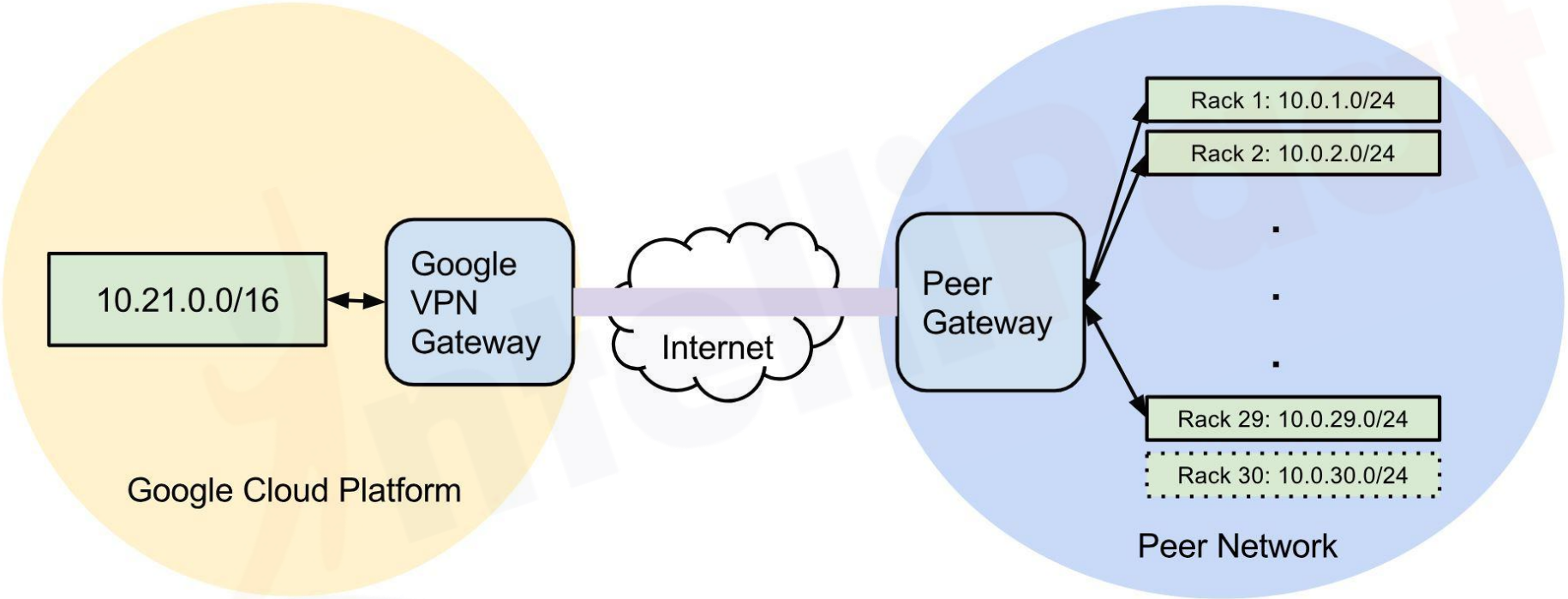
Typical VPN Setup



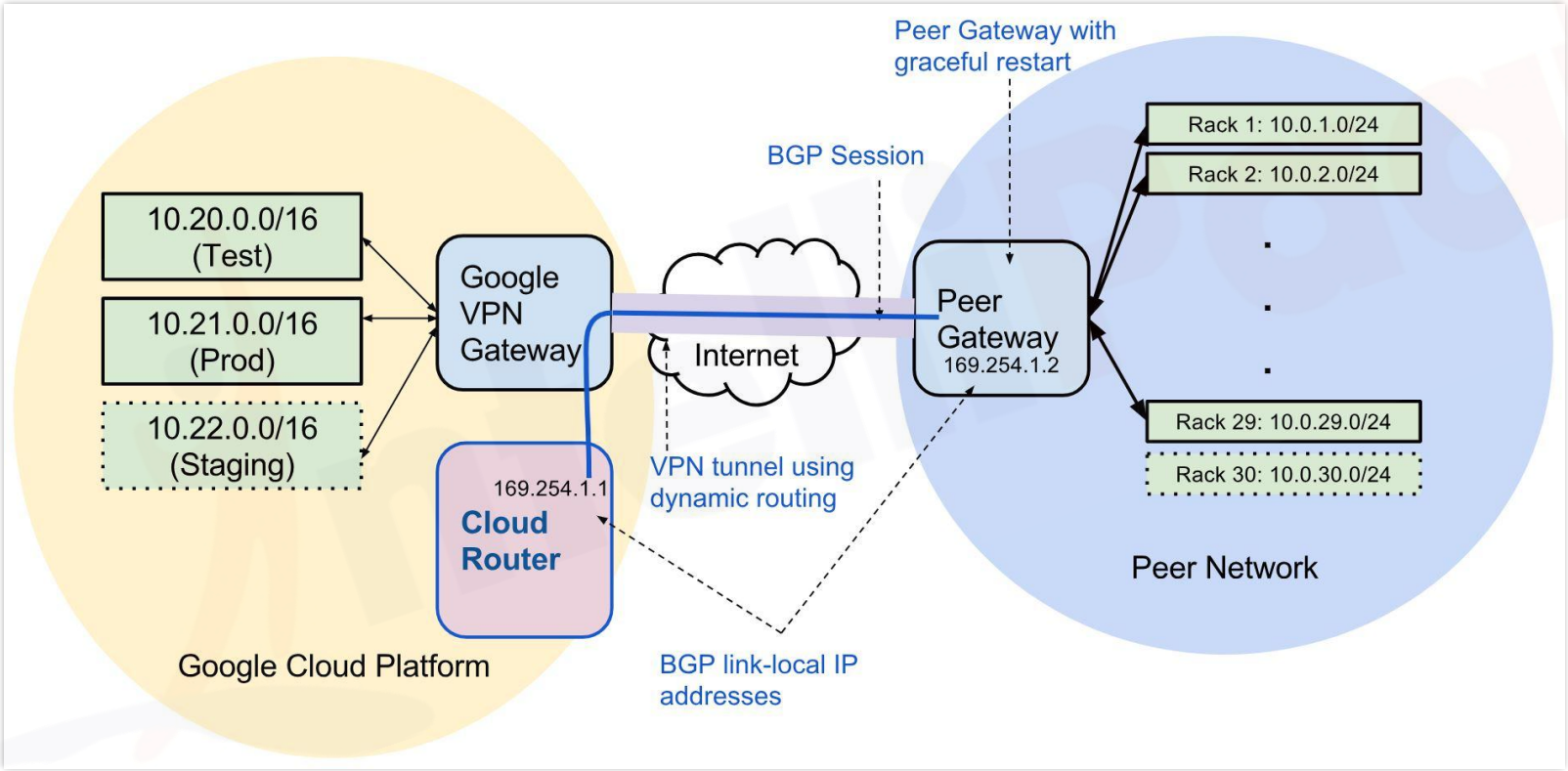
Cloud VPN



Static Route

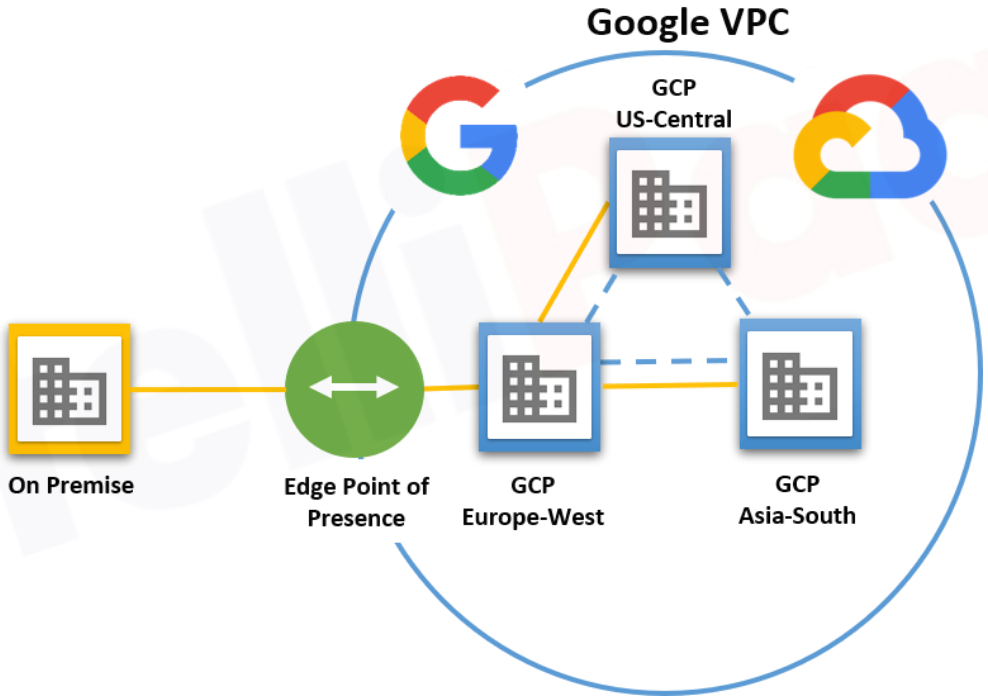


Cloud Router

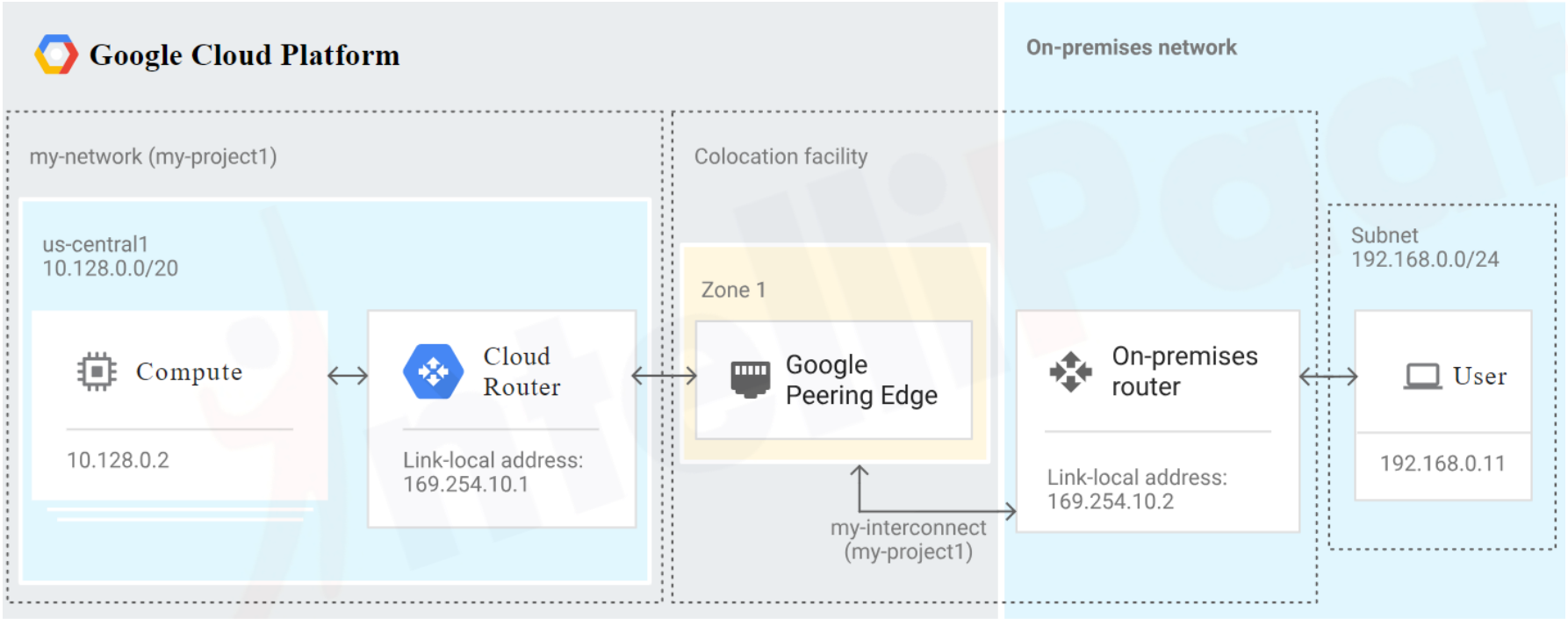


Cloud Interconnect

- Dedicated Interconnect
- Partner Interconnect



Dedicated Interconnect



Source: https://cloud.google.com/interconnect/docs/concepts/dedicated-overview

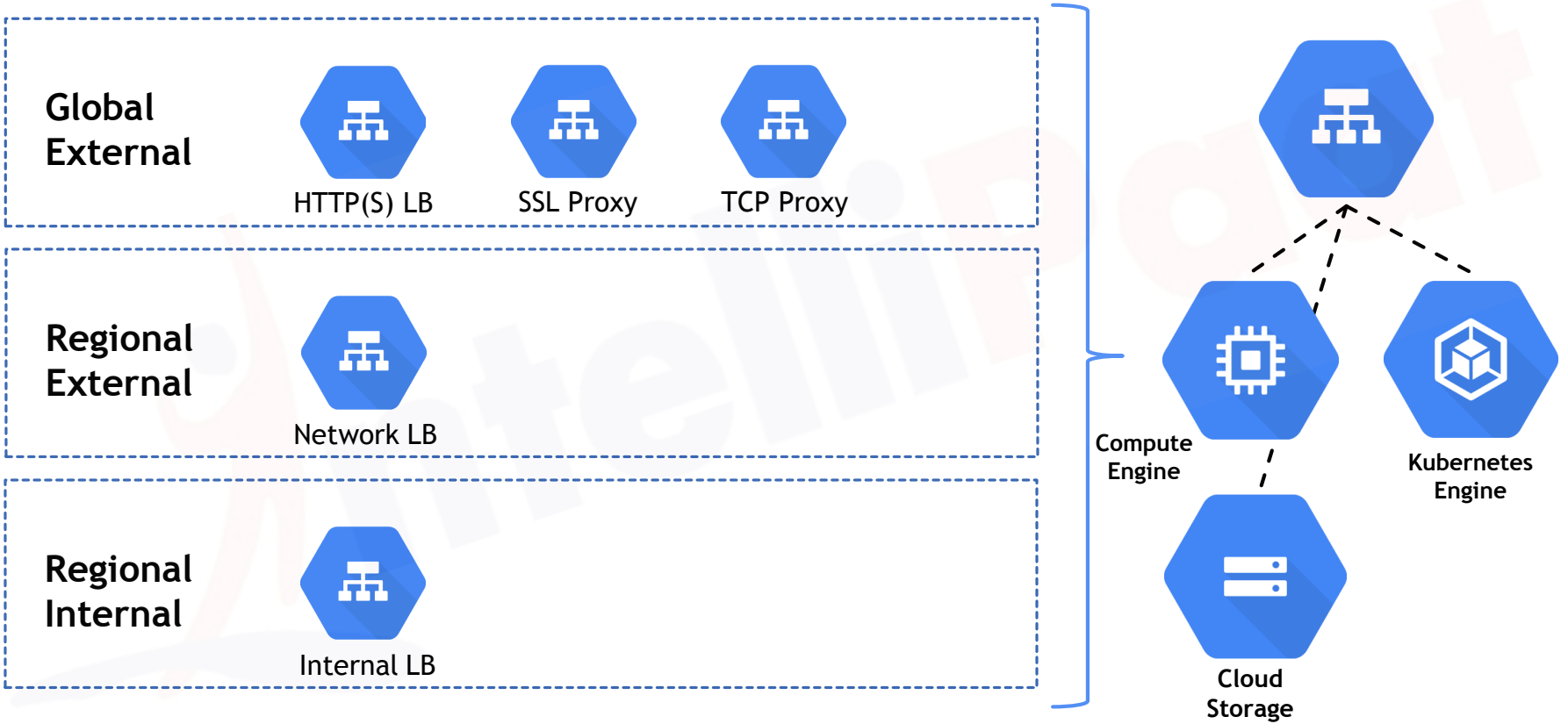
Cloud VPN Vs Dedicated Interconnect Vs Direct Peering

Feature	Cloud VPN	Interconnect	Peering
Access Type	Internal IP address - RFC 1918 address space	Internal IP address - RFC 1918 address space	Public IP addresses
Capacity	1.5 - 3 Gbps per tunnel over an encrypted public internet	**Dedicated Interconnect**: 10 Gbps per link. With up to eight connections per interconnect, you have 80 Gbps	**Direct Peering**: 10 Gbps per link.
Capacity Partner	-	**Partner Interconnect**: 50 Mbps,100-500 Mbps & 1,2,5,10 Gbps	Carrier Peering: Contact the Network Provider
Price	▪ Egress rate ▪ Number of Tunnels	▪ Egress rate ▪ Fee for VLAN	• Egress rate • Establishing a direct peering connection with Google is free
SLA	99.9%	99.99%	No SLA
OSI Layer	Layer 3	Layer 2	Layer 3

Open Systems Interconnection (OSI) model

Layers	Description & Protocols
Application (L7)	▪ End User Layer ▪ **HTTP(S)**, FTP, SSH, DNS
Presentation (L6)	▪ Syntax Layer ▪ SSL, SSH, IMAP, FTP, MPEG, JPEG
Session (L5)	▪ Synch & Send to Port ▪ API's, Sockets, Winsock
Transport (L4)	▪ End-to-end connection ▪ **TCP(Transmission Control Protocol), UDP (User Datagram Protocol)**
Network (L3)	▪ Packets ▪ IP (IPv4, IPv6), ICMP, **IPSec**
Data Link (L2)	▪ Frames ▪ **Ethernet**
Physical (L1)	▪ Physical structure ▪ Coax, Fiber, Repeaters

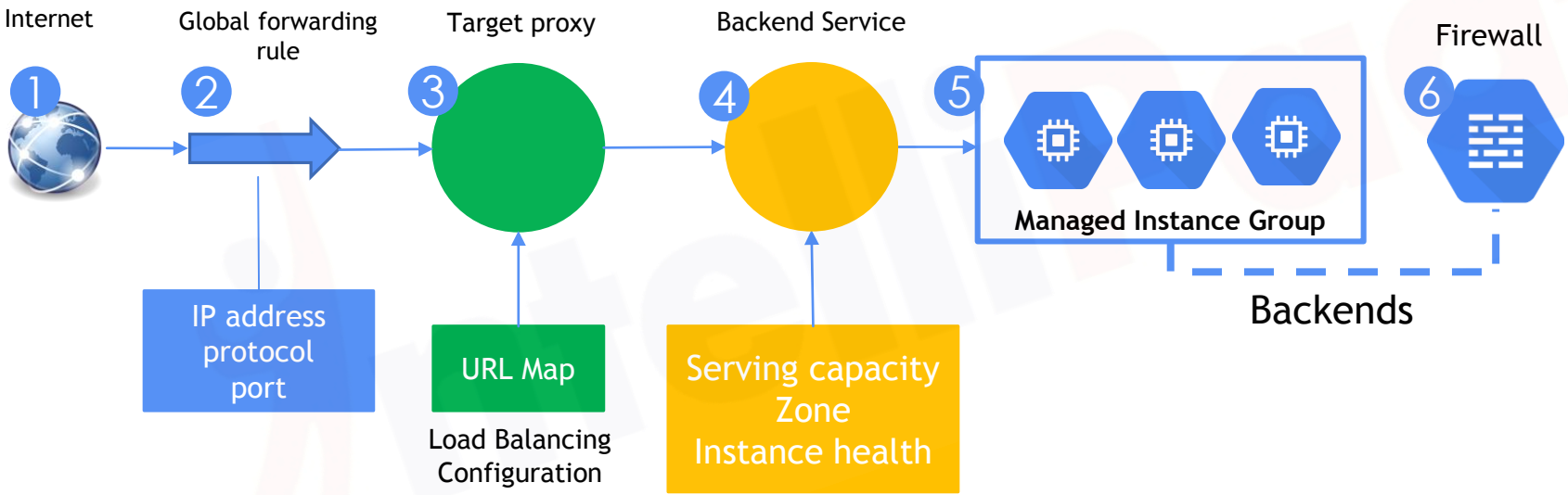
Cloud Load Balancer



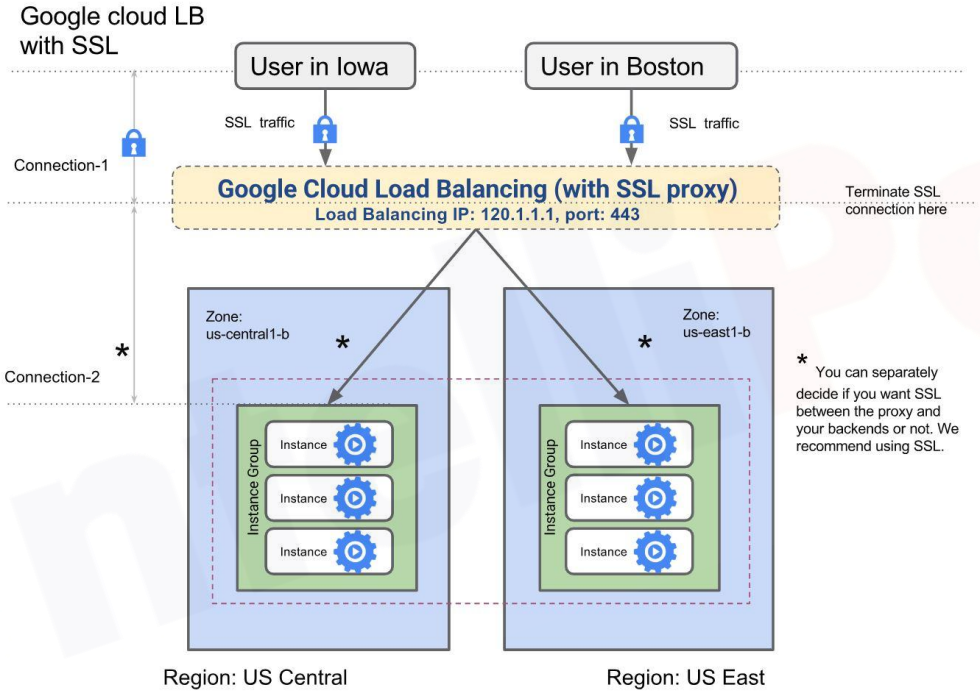
Cloud Load Balancer

Load Balancer	Traffic Type	Global/ Region	External/ Internal	Ports
HTTP(S)	HTTP/ HTTPS	Global	External	80, 8080, 443
SSL Proxy	TCP with SSL Offload	Global	External	25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, and 5222
TCP Proxy	TCP without SSL offload. **Does not preserve client IP addresses**	Global	External	25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, and 5222
Network TCP/ UDP	TCP/UDP without SSL offload. **Preserves client IP addresses**	Regional	External	Any
Internal TCP/ UDP	TCP/ UDP	Regional	Internal	Any

Global HTTP(S) Load Balancing

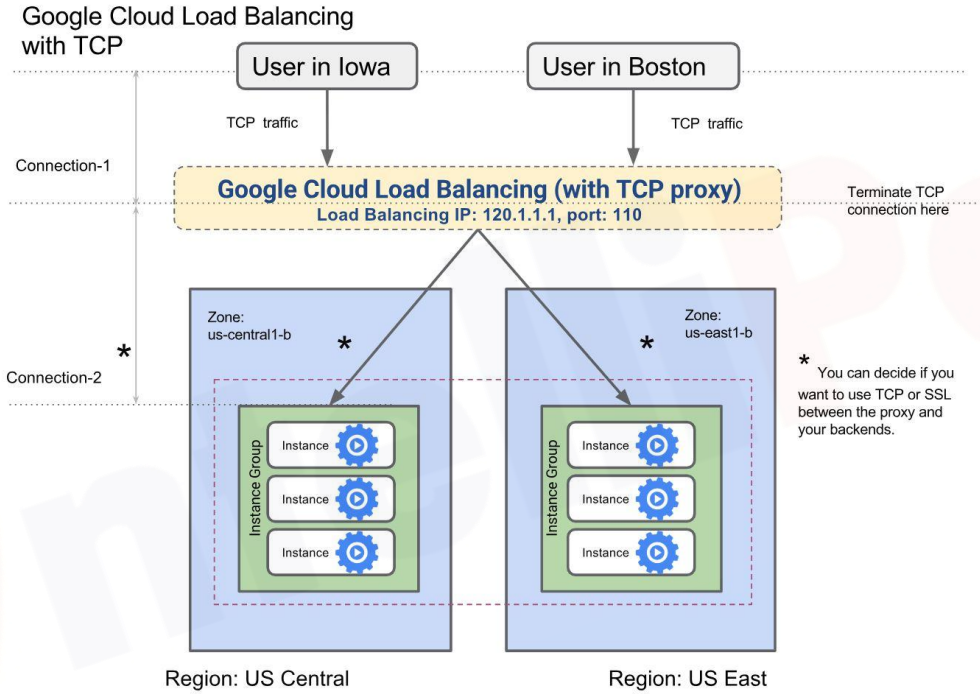


Load Balancing with SSL Proxy



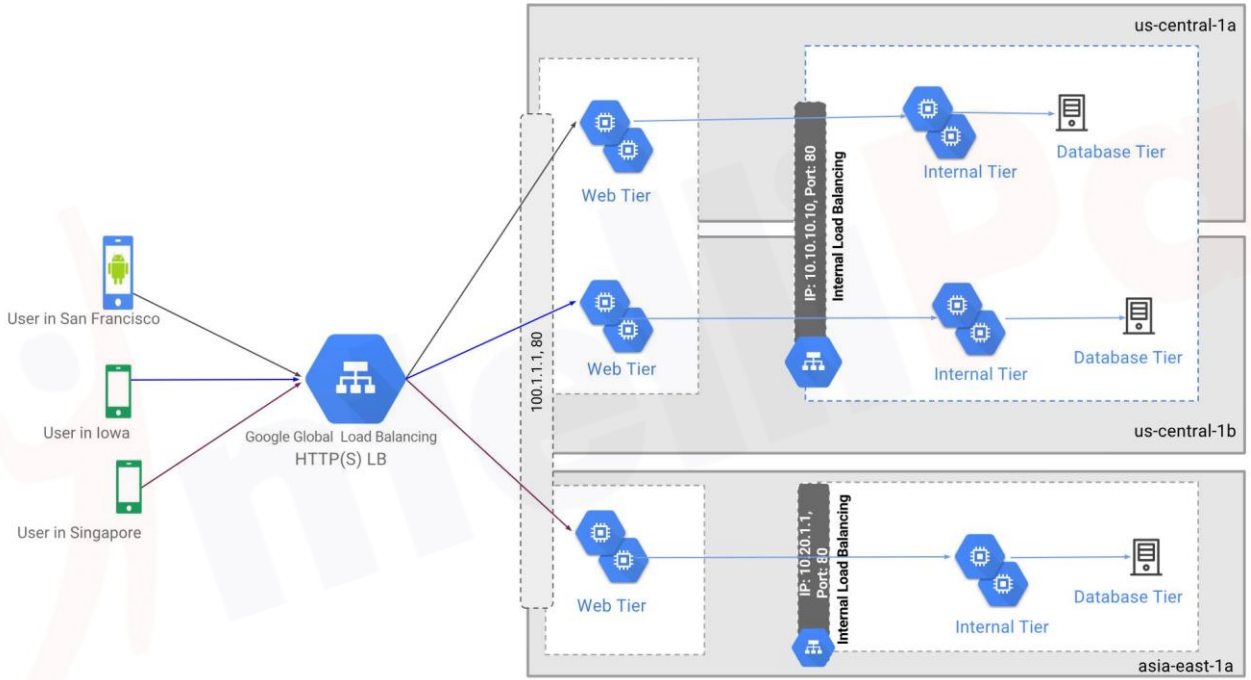
Source: https://cloud.google.com/load-balancing/docs/ssl/

Load Balancing with TCP Proxy



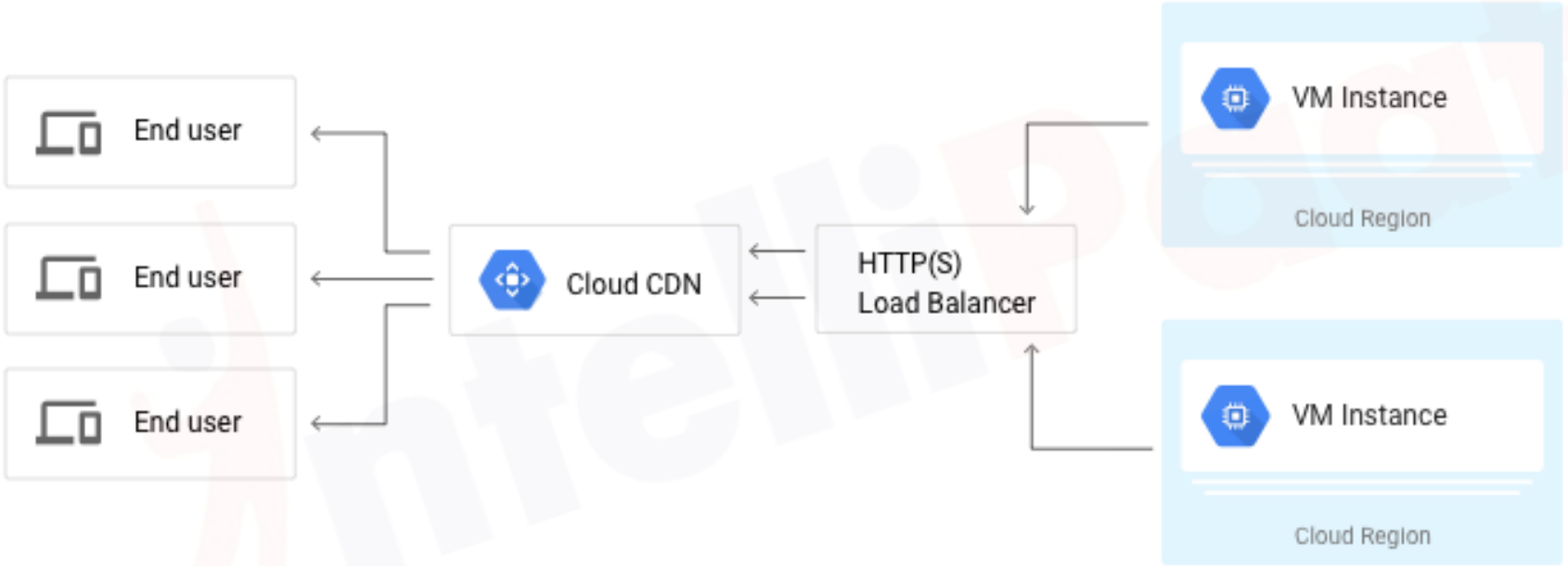
Source: https://cloud.google.com/load-balancing/docs/tcp/

Global HTTP LB + Internal LB in action



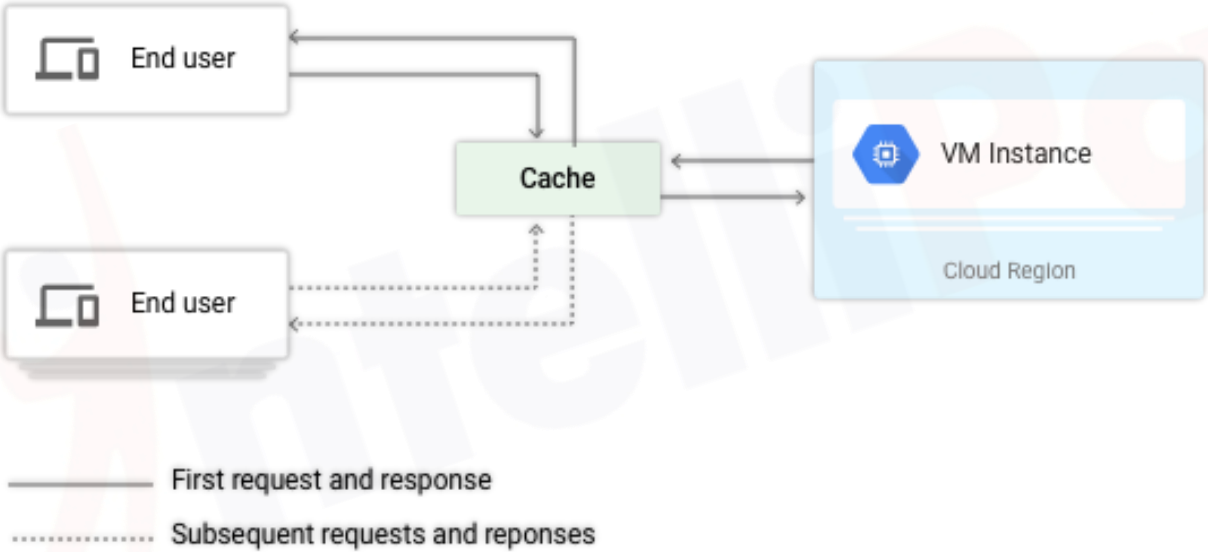
Source: https://cloud.google.com/load-balancing/docs/internal/

Cloud CDN



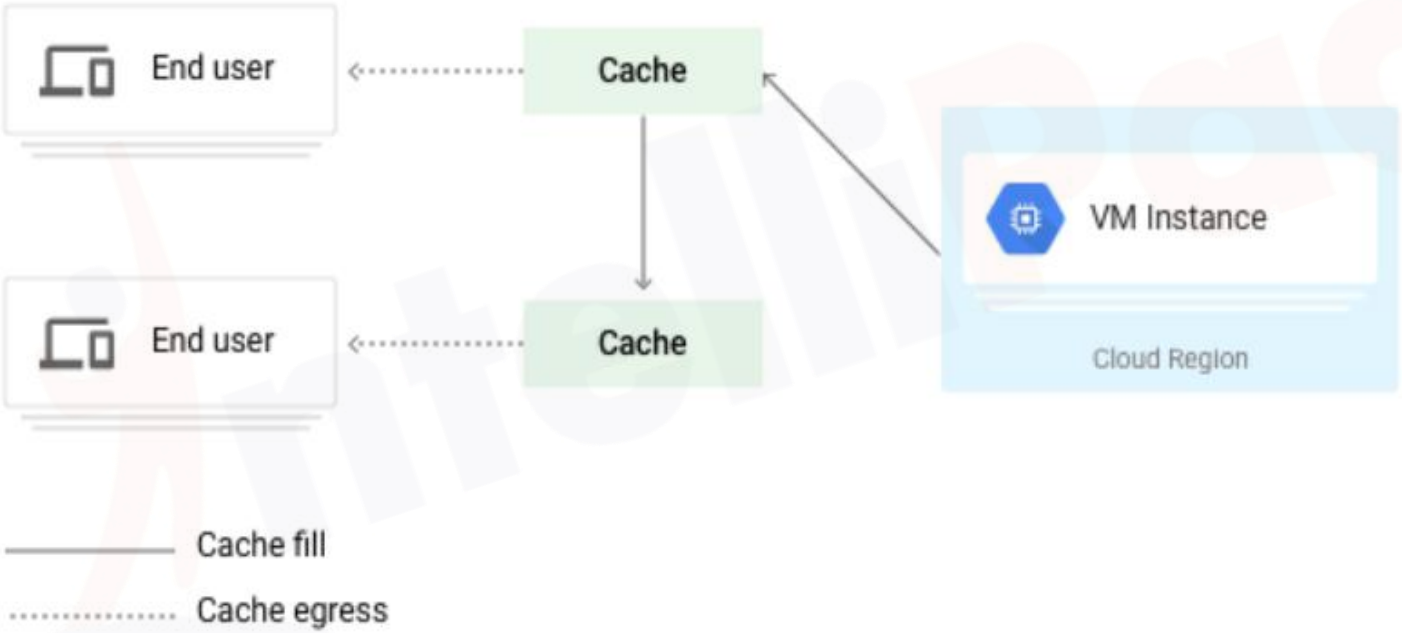
Source: https://cloud.google.com/cdn/docs/overview

Cloud CDN - Cache miss and cache hit



Source: https://cloud.google.com/cdn/docs/overview

Cloud CDN - Cache fill and cache egress



Source: https://cloud.google.com/cdn/docs/overview

QUIZ

Quiz 1

Your company is building a large-scale web application. Each team is responsible for its own service components of the application and wants to manage its own individual projects. You want each service to communicate with the others over RFC1918 address space. What should you do?

A	Deploy each service into a single project within the same VPC.
B	Configure Shared VPC and add each project as a service of the Shared VPC Project.
C	Configure each service to communicate with the others over HTTPS protocol.
D	Configure a global load balancer for each project, and communicate between each service using the global load balancer IP addresses

Answer 1

Your company is building a large-scale web application. Each team is responsible for its own service components of the application and wants to manage its own individual projects. You want each service to communicate with the others over RFC1918 address space. What should you do?

A	Deploy each service into a single project within the same VPC.
B	Configure Shared VPC and add each project as a service of the Shared VPC Project.
C	Configure each service to communicate with the others over HTTPS protocol.
D	Configure a global load balancer for each project, and communicate between each service using the global load balancer IP addresses

Quiz 2

How many more VPCs can one Project have if it already having default VPC?

A	4
B	5
C	3
D	10

Answer 2

What are Virtual Machine scale sets in Azure?

A	4
B	5
C	3
D	10

Quiz 3

A customer wants 20 gigabits per second (Gb/s) capacity/ bandwidth between their data centre and GCP. Which option suits their requirement?

A	Cloud VPN
B	Partner Interconnect
C	Cloud Router
D	Dedicated Interconnect

Answer 3

A customer wants 20 gigabits per second (Gb/s) capacity/ bandwidth between their data centre and GCP. Which option suits their requirement?

A	Cloud VPN
B	Partner Interconnect
C	Cloud Router
D	Dedicated Interconnect

Quiz 4

Organization A & B both uses GCP for building their applications. Both wants to leverage GCP infrastructure and reduce egress cost. What is the best option for applications in organization A to communicate with applications in organization B?

A	VPC Peering
B	Shared VPC
C	Create a custom VPC
D	Applications in two organization can communicate each with zero configuration and setup

Answer 4

Organization A & B both uses GCP for building their applications. Both wants to leverage GCP infrastructure and reduce egress cost. What is the best option for applications in organization A to communicate with applications in organization B?

A	VPC Peering
B	Shared VPC
C	Create a custom VPC
D	Applications in two organization can communicate each with zero configuration and setup

IntelliPaat

India : +91-7847955955

US : 1-800-216-8930 (TOLL FREE)

sales@intellipaat.com

24X7 Chat with our Course Advisor