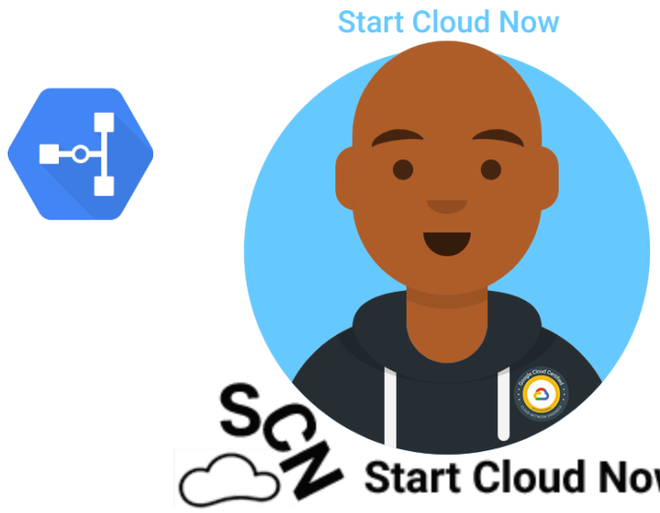
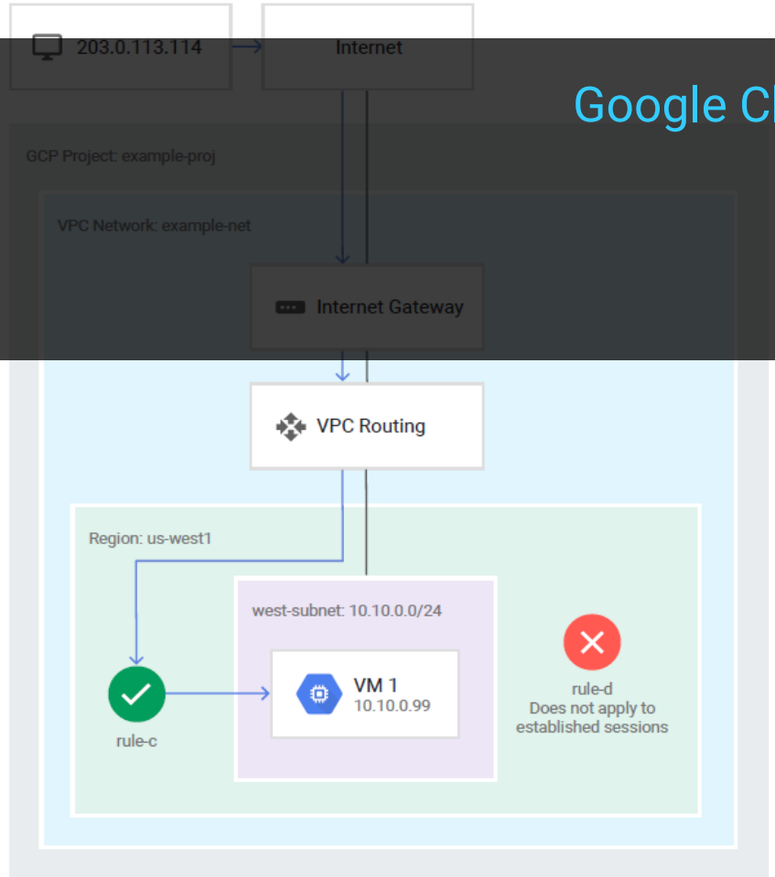




Google Cloud Professional Cloud Network Engineer Exam

Prep Notes by

Ammett

V1.2

Google Cloud Platform

Google Cloud Professional Cloud Network Engineer

Exam Prep Sheet by Ammett

This is my guide based on my preparation for the exam. References from Google Docs and other sources.

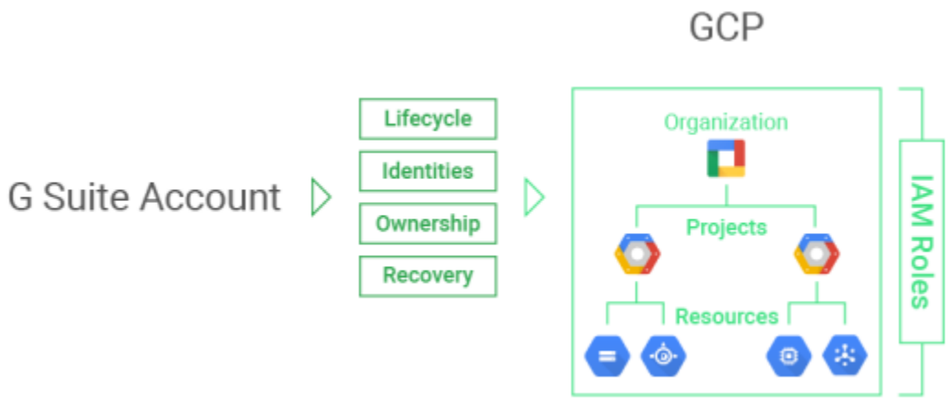
V1.2: 01-2020

White papers you must review

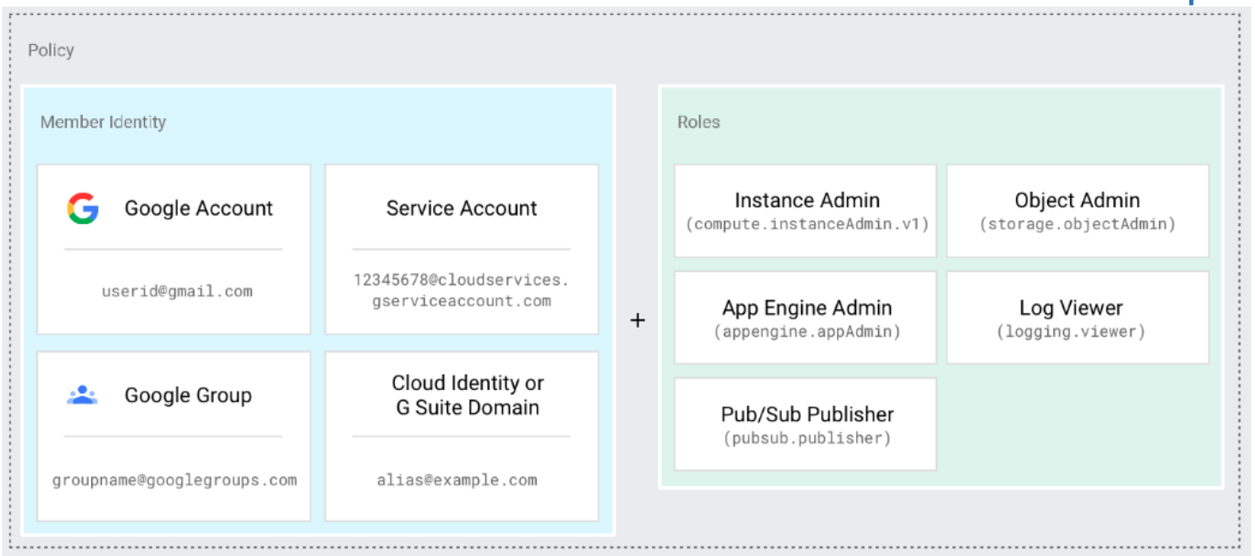
1-Best practices for enterprise organizations
2- VPC Overview
3- Alias IP
4- VPC Network Peering
5- Shared VPC
6- Choosing a load balancer
7- Cloud CDN Overview
8- Choosing a VPN option
9- Cloud Router
10- Direct Peering
11- Carrier peering
12- Dedicated Interconnect
13- Partner Interconnect
14- Creating a VPC-native Cluster
15- Private Cluster Kubernetes
16- Firewall Rules Logging
17- Cloud DNS
18- Networking Kubernetes
19- URL_Map
20- Load balancer health checks

Organisation Structures	**What it is** Resources are organized hierarchically. This allows you to map your enterprise's operational structure to GCP, and to manage access control and permissions for groups of related resources.	**Key points** 1- Flow (Organisation, Folders, Projects, Resources) 2- Where to manage permissions for groups, department, entire organisation, etc	**What you should know** 1- Permissions level necessary to do certain functions 2- Domains, Groups, G Suite domain, Super users.	**Review documents** Cloud Platform hierarchy	**Video** Hierarchy	**My experience** This area is fundamental please understand how to control to get the separation and security in your domain.
Cloud IAM	**What it is** IAM which lets you manage access control by defining who (identity) has what access (role) for which resource.	**Key points** 1- Best way to manage (use groups) 2- Roles (primitive, predefined & custom) 3- Roles necessary to do certain functions (network, security, IAM, cloud storage)	**What you should know** 1- Permissions level necessary 2- Permission errors 3- How & when to create custom roles 4- Service account permissions	**Review documents** Cloud IAM overview	**Video** Cloud IAM Best practices for identity	**My experience** IAM on a networking exam? Yes, know it well because it will come. Knowing the roles necessary for certain actions may help if you can figure it out.
CIDR RFC-1918	**What it is** You can choose any private RFC 1918 CIDR block for the primary IP address range of the subnet	**Key points** 1- The 4 Reserved Address (network, gateway, google reserved, broadcast) 2- How to assign your own range	**What you should know** 1- How to assign static internal IP 2- How to change IP	**Review documents** IP Addresses Reserve Internal IP	**Video** Networking with IP Address	**My experience** Some form of RFC-1918 will come. Keep in mind what is reserved, auto-mode RFC 1918 addresses.
External IP	**What it is** These are routable on the public internet and allow you access to the internet.	**Key points** 1- This is optional 2- Default is ephemeral-these change 3- Static can be assigned 3- How to create static external IP	**What you should know** 1- Charged if not attached to VM 2- How to change ephemeral IP to another ephemeral IP	**Review documents** Reserve External IP		**My experience** These can appear but shouldn't be too difficult to handle
Subnet Types	**What it is** Subnets are used to separate resources and control communication between tiers. Access can be controlled via routes and firewalls	**Key points** 1- Default (automatically generated with a project) they have default firewall rules and a subnet in every region 2- Auto-mode- automatically creates a subnet in every region (the default subnet is an auto mode subnet) IP range 10.128.0.0/9	**What you should know** 1- Custom is fully user controlled 2- Avoid overlapping ranges 3- You can convert from auto to custom (one way). Things can get affected. 4- You can increase range not decrease		**Video** Create Custom Subnet	**My experience** Take note of this area. CIDR block host availability for VPC and also in Kubernetes.
Private Access	**What it is** Allows VM with internal (RFC 1918) IP addresses to reach certain APIs and services without internet access.	**Key points** 1- No public IP address 2- Enabled on subnet 3- Default route	**What you should know** 1- Services that support Private access 2- Default route 0.0.0.0/0 next hop " default internet gateway" or custom routes 199.36.153.4/30 or 199.36.153.8/30 nexthop "default internet gateway"	**Review documents** Private Google Access	**Video** Access GCP and 3rd party services privately	**My experience** This is a **key topic.** Especially what services are supported and how to set up.

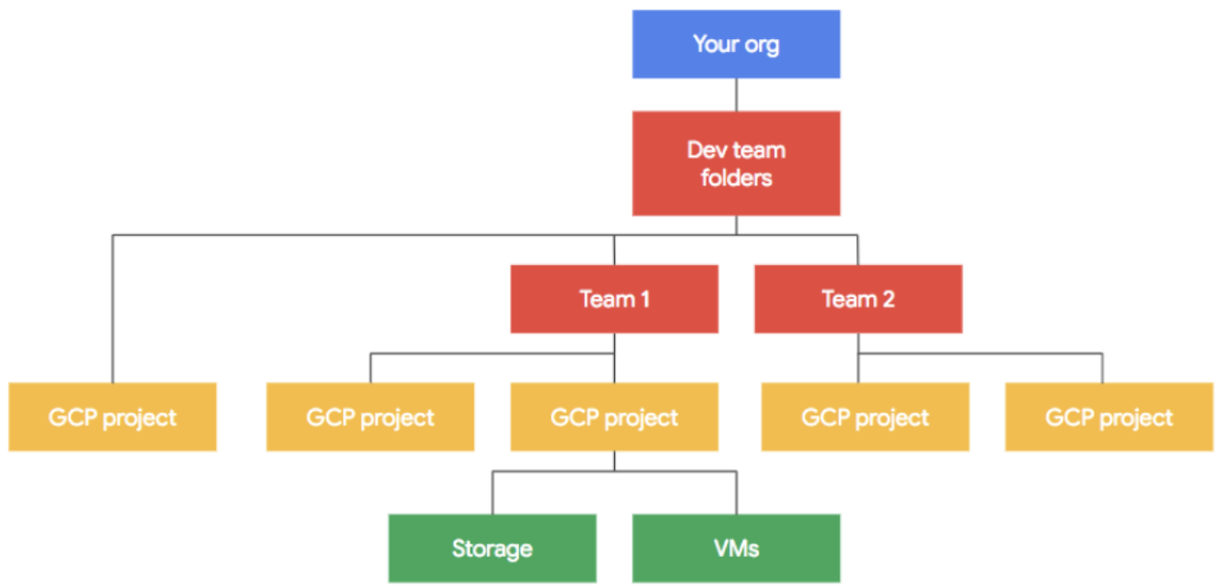
IAM example 1



IAM example 2



Hierarchy Flow

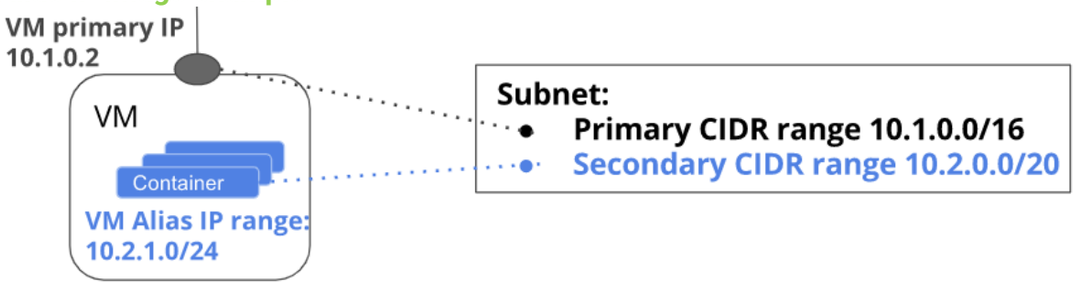


Reserved range example

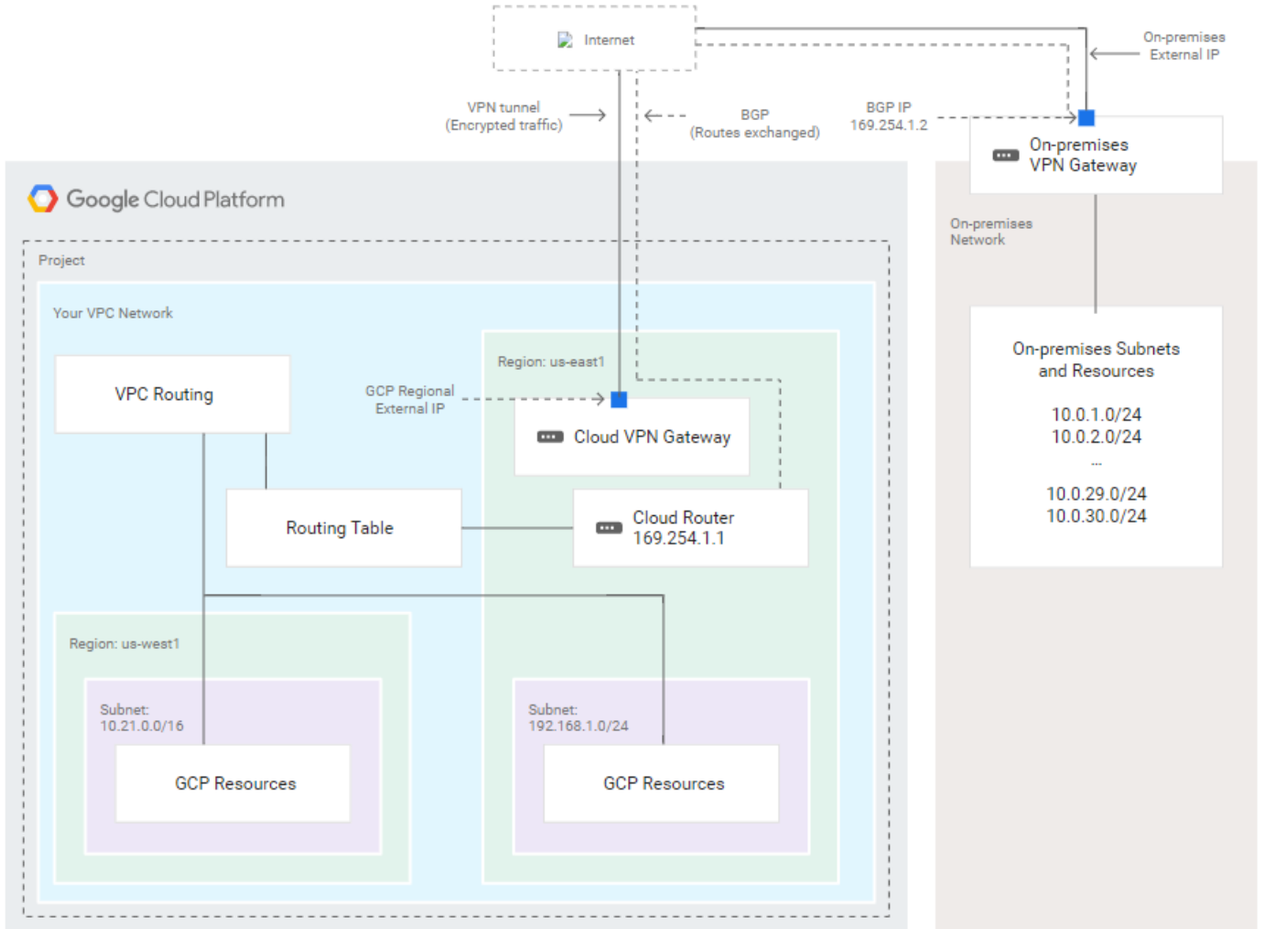
Reserved Address	Description	Example
Network	First address in the primary IP range for the subnet	`10.1.2.0` in `10.1.2.0/24`
Default gateway	Second address in the primary IP range for the subnet	`10.1.2.1` in `10.1.2.0/24`
Second-to-last address	Second-to-last address in the primary IP range for the subnet that is reserved by GCP 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`

Private Service	**What it is** The private connection enables VM in your VPC network and the services that you access to communicate exclusively by using internal (RFC 1918) IP addresses.	**Key points** 1- External IP addresses are not required or used 2- Service producers network 3- Private IP 4- **Cloud SQL** supports this	**What you should know** 1- Works via peering from customer to service producer network 2- Must define CIDR range for services. 3- Connect within same region	**Review documents** Config private service access	**Video** Access GCP and 3rd party services privately	**My experience** Know difference between Private services and Private access. Know which services use which.
Alias IP	**What it is** Alias IP ranges let you assign ranges of internal IP addresses as aliases to a (VM) nic. This is useful if you have multiple services running on a VM and you want to assign each service a different IP address. Alias IP ranges also work with GKE Pods.	**Key points** 1- Main address from primary CIDR 2- Alias can be from main CIDR or 3- Alias IP can be from secondary rages.	**What you should know** 1- Use of alias IP ranges does not require secondary subnet ranges. These secondary subnet ranges merely provide an organizational tool.	**Review documents** Alias IP Configuring Alias IP		**My experience** Pay attention here. Alias IP can be used in VM and Kubernetes.
VPC	**What it is** A VPC network is your virtual network in the cloud just like an on premise physical network or data centre or office network.	**Key points** 1- **VPC are global** SDN 2- How to get traffic flowing 3- Using RFC 1918 subnets 4- **Internal and external** access	**What you should know** 1- Internal and external access 2- Controlling access and firewalls 3- How to Connect VPC together (peering or sharing)	**Review documents** VPC Overview	**Video** VPC Deep Dive	**My experience** **Core area**. Let me put it like this; If you do not understand all of the elements of a VPC; then don't do the exam.
Routes	**What it is** These define the paths network traffic takes from a VM instance to other destinations. These destinations can be inside or outside of your VPC.	**Key points** 1- The route table is defined at network level 2- The routing to next hop where should the next hop be	**What you should know** 1- Type (system and custom) 2- Default route & Subnet route 3- Static and Dynamic routes 4- Routing order	**Review documents** Routes in GCP	**Video** Cloud Router	**My experience** You cannot have networking without routes. (Static, dynamic, subnet, custom, default, import, export)
Cloud Router	**What it is** This enables you too dynamically exchange routes between (VPC) and on-premises networks by using Border Gateway Protocol (BGP).	**Key points** 1- Cloud Router automatically learns new subnets in your VPC network and announces them to your on-premises network	**What you should know** 1- Global dynamic routing 2- Regional dynamic routing	**Review documents** Cloud Router		**My experience** Another critical area. Know how these are setup. Has lot of small parts get familiar.
BGP	**What it is** Border Gateway Protocol is a protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers.	**Key points** 1- The ASN number range (64512 - 65534, 4200000000 – 4294967294) 2- IP range used 169.254.0.0/16	**What you should know** 1- **MED** (route priority) 2- What can be configured without BGP 3- Troubleshooting	**Review documents** Establishing BGP sessions Troubleshooting Cloud Router		**My experience** A question or 3 may come on BGP. Know what is required, problems and how it works.
Firewall	**What it is** Allow or deny traffic to and from your virtual machine (VM) etc, based on configurations you specify.	**Key points** 1- How they work (Stateful) & Scope 2- Implied rules 3- Default rules	**What you should know** 1- How to restrict traffic	**Review documents** Firewalls	**Video** Firewalls Network and security telemetry	**My experience** You can't allow everything on your network so expect a few firewall questions in the networking exam also.
Firewall logging	**What it is** **Firewall Rules Logging** allows you audit, verify, and analyze the effects of your firewall rules.	**Key points** 1- Individually enabled 2- Supported for TCP & UDP only 3- Cannot enable on implied or default rules	**What you should know** 1- Troubleshooting viewing (Log entries missing, cannot view logs, where to apply logs)	**Review documents** Firewall Logging		**My experience** You should have an idea where to look, what rules are logged, priorities and how to fix.

Alias IP image example



Cloud Router for VPNs with VPC network



Trouble shooting logs

Log entries missing

Possible cause: Connections might not match the firewall rule you expect

Verify that the firewall rule you expect is in the list of applicable firewall rules for an instance. Use the GCP Console to view details for the relevant instance, then click the **View details** button in the *Network interfaces* section on its *VM instance details* page. Inspect applicable firewall rules in the *Firewall rules and routes details* section of its *Network interface details* page.

Review the firewall rules overview to make sure you have created your firewall rules correctly.

You can use tcpdump on the VM to determine if connections it sends or receives have addresses, ports, and protocols that would match the firewall you expect.

Possible cause: A higher priority rule with firewall rules logging disabled might apply

Firewall rules are evaluated according to their priorities. From the perspective of a VM instance, only one firewall rule applies to the traffic.

A rule that you think would be the highest priority applicable rule might not actually be the highest priority applicable rule. A higher priority rule that does not have logging enabled might apply instead.

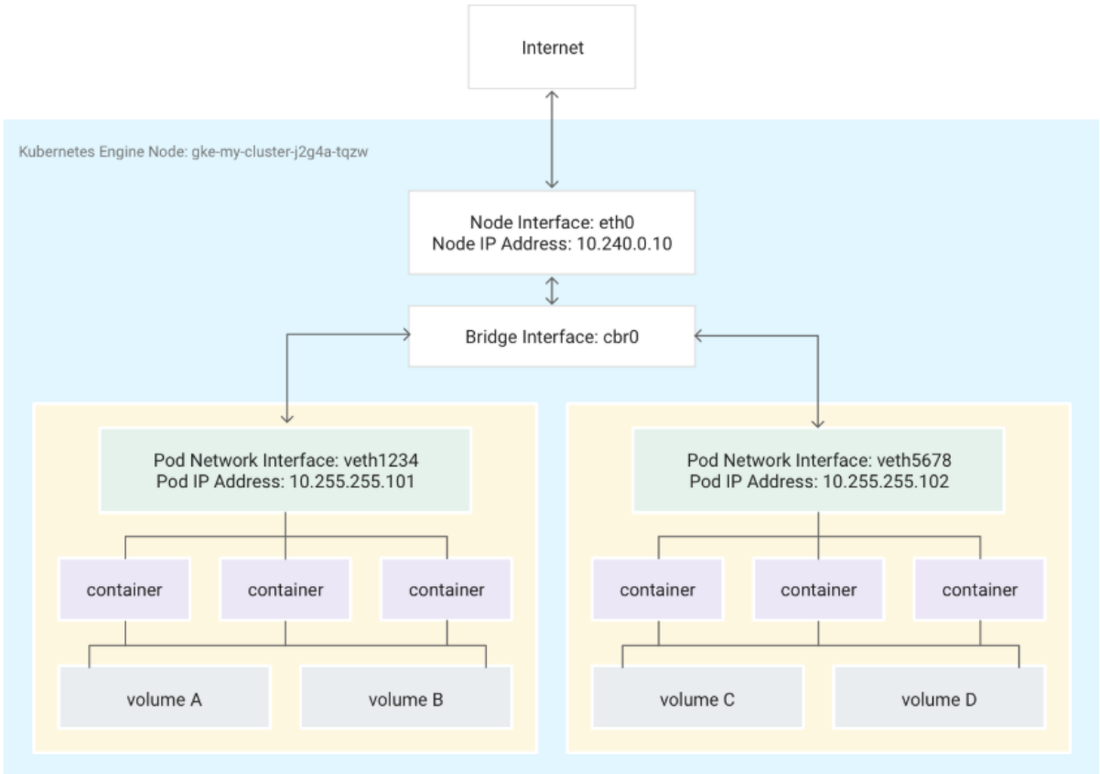
To troubleshoot, you can temporarily enable logging for *all* possible firewall rules applicable to a VM. Use the GCP Console to view details for the relevant VM, then click the **View details** button in the *Network interfaces* section on its *VM instance details* page. Inspect applicable firewall rules in the *Firewall rules and routes details* section of its *Network interface details* page, and identify your custom rules in that list. Temporarily enable logging for all of those custom firewall rules.

With logging enabled, you can identify the applicable rule. Once identified, be sure to disable logging for all rules that do not actually need it.

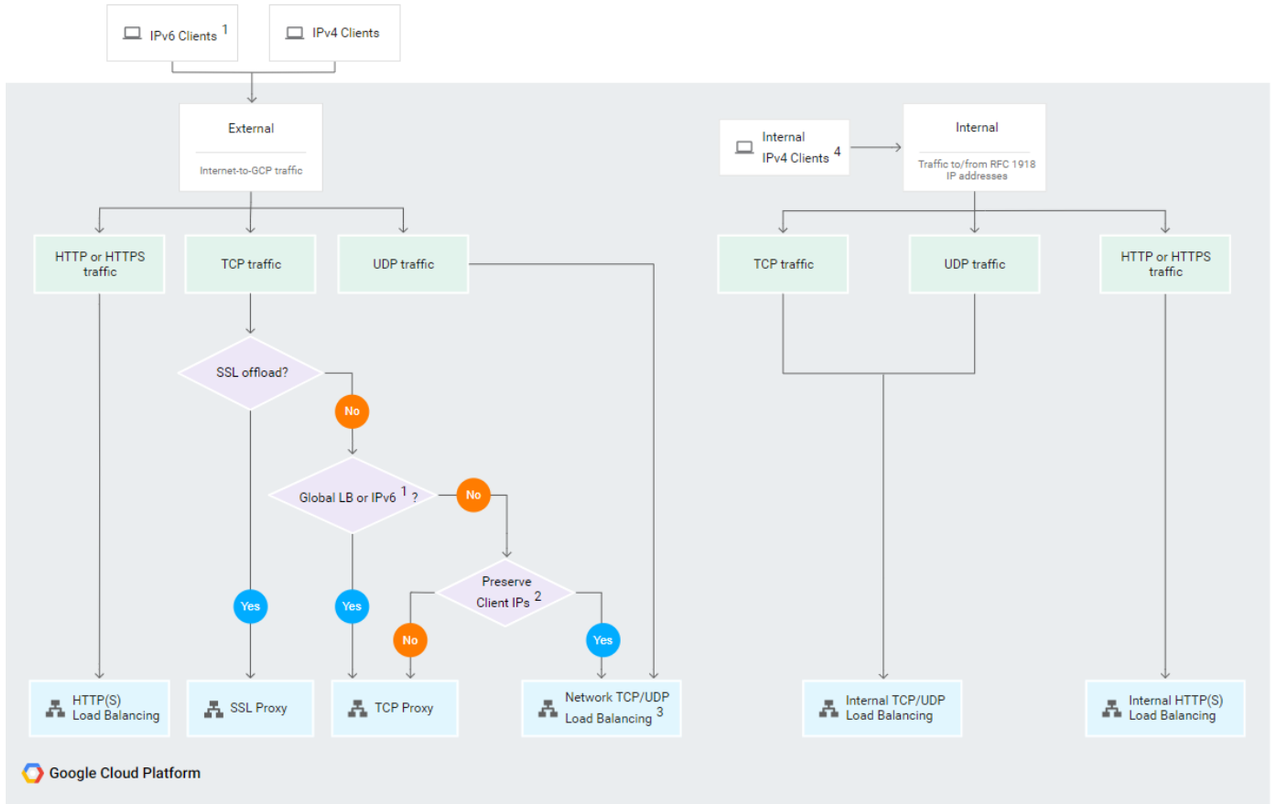
HTTP(S) Load balancer	SSL Proxy	TCP Proxy	Network Load balancer	Internal load balancer	Kubernetes Load balancing	**Review documents** Choosing a load balanced Troubleshooting health HTTPS logging Kubernetes HTTP(s) LB ingress
What it is Load balancer for HTTP(S) traffic, global, external, 80 or 8080 on 443.	**What it is** Load balancer for TCP with SSL offload, global, external. (25, 43, 110, 143,195, 443, 465, 587, 700, 993, 995, 1883, and 5222)	**What it is** Load balancer for TCP without SSL, global, external. (25, 43, 110, 143,195, 443, 465, 587, 700, 993, 995, 1883, and 5222)	**What it is** Load balancer for TCP/UDP no SSL offload, regional, external. (any port)	**What it is** Load balancer for TCP /UDP regional, Internal traffic (any port)	**What it is** This allows you balance between you application running in Kubernetes	Setting up HTTP Ingress LB **Video** Cloud Load balancers **My experience** **Loads and loads** of variation on this area. (**Global** vs **Regional**, External vs Internal, **Traffic type**, VoIP, TFTP, IP, TCP, UDP). Understand health checks checks. For Kubernetes understand connection points of load balancers. If you don't understand these don't do the exam.
What you should know 1- Scope global 2- HTTPS traffic 3- Health checks	**What you should know** 1- Scope Global 2- Non HTTPS traffic with SSL termination	**What you should know** 1- Scope Global 2- TCP/UDP traffic 3- Health checks	**What you should know** 1- Scope regional 2- TCP/UDP traffic 3- Health checks	**What you should know** 1- Scope Regional 2- Internal TCP/UDP traffic	**What you should know** 1- How it works 2- Connections points 3- Type of LB supported (HTTPS-**Ingress**, Internal, External)	
Key Points 1- Services that need HTTPS Load balancing	**Key Points** 1- SSL termination	**Key Points** 1- Scope global	**Key Points** 1- Scope global 2- HTTPS traffic	**Key Points** 1- Scope global 2- HTTPS traffic	**Key Points** 1- What IP you connect to 2- HTTPS traffic	

DDoS	URL-Mapping	Managed Instance Groups	Unmanaged Instance Groups	Canary Deployments	Rolling Deployments	**Review documents** Rolling Updates Managed instances Unmanaged instances URL_Map
What it is A (DDoS) attack is a malicious attempt to disrupt normal traffic to a targeted service or network by overwhelming the target infrastructure with a flood of Internet traffic.	**What it is** Google Cloud Platform HTTP(S) load balancers use a URL map to direct incoming requests to backend services and backend buckets.	**What it is** A managed instance group contains identical instances that you can manage as a single entity in a single zone.	**What it is** Unmanaged instance groups are collections of instances that are not necessarily identical and do not share a common instance template.	**What it is** A canary update is an update that **is applied** to a partial number of instances in the instance group.	**What it is** A rolling update is an update that is gradually applied to all instances in an instance group until all instances have been updated	**Video** Highly available deployments
What you should know 1- How to prevent with GCP tools	**What you should know** 1- How to configure 2- It works with HTTPS LB's	**What you should know** 1- Global 2- TCP/UDP traffic 3- Health checks	**What you should know** 1- When to use. 2- Different template.	**What you should know** 1- Applies to a defined amount or % of host	**What you should know** 1- Applies to 100% of the target as defined 2- You can configure time etc	
Key Points 1- Traffic controlling tools is necessary	**Key Points** 1- Hostname and path 2- Characters / an *	**Key Points** 1- Managed instance groups support Autoscaling, load balancing, rolling updates, autohealing, and more.	**Key Points** 1- Unmanaged groups do not create, delete, or scale the number of instances in the group.	**Key Points** 1- Understand when to use for minimization of application performance issues	**Key Points** 1- Understand when to use and impact on application performance	**My experience** All these area combined made for some **VERY** challenging questions. Kubernetes is well represented, learn networking, subnetting and load balancing well.

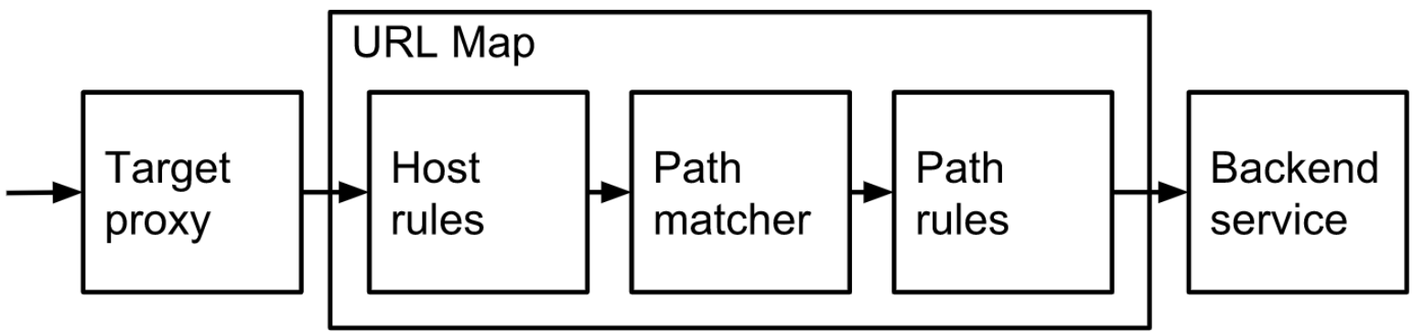
Kubernetes networking example



Choosing a Load balancer diagram



URL Map example

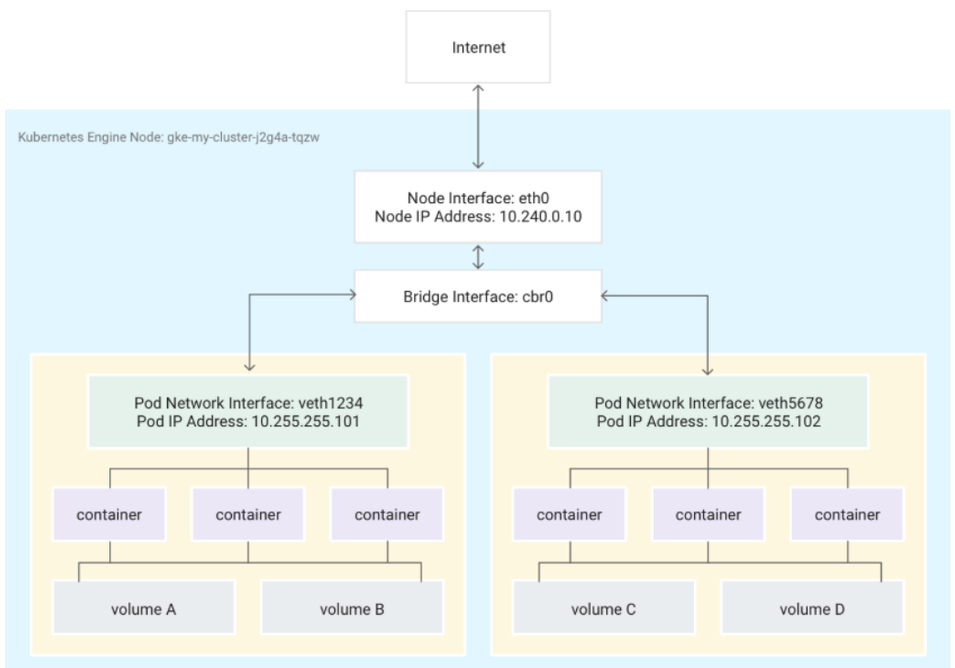


Google Kubernetes Engine	Cluster	Node	Pods	IP tables	Kubernetes subnetting	**Review documents** Networking in Kubernetes
What it is GKE provides a managed environment for deploying, managing, and scaling your containerized applications using Google infrastructure.	**What it is** A cluster consists of at least one **cluster master** and multiple nodes. These master and node machines run the Kubernetes cluster orchestration system	**What it is** They are the worker machines that run your containerized applications and workloads Each node is managed from the master.	**What it is** **Pods** are the smallest, most basic deployable objects in Kubernetes. Pods contain one or more *containers*,	**What it is** Kube-proxy manages the iptables rules on the node.	**What it is** IP addresses are used for Pods, Nodes and services. The IP subbnetting scheme must take into consideration enough for expansion.	**Video** Deep dive Into Kubernetes Networking **My experience** Kubernetes is represented as it should be on this exam. Pay attention to the networking components, subnetting and structure.
What you should know 1- IP (Cluster, Pod, Node) 2- IP allocation to (nodes, pods, services) 3- Health checks	**What you should know** 1- Kubernetes object all run on top a cluster 2- Cluster master runs control plane, API server, scheduler and resource controllers.	**What you should know** 1- You can run a maximum of 110 Pods on a node with a /24 range. 2- Node run kubelet and services to support Docker containers. 3- IP assigned from primary range.	**What you should know** 1- Pods are ephemeral. 2- Pods do not "heal" or repair themselves. 3- Containers in a pod communicate via local host 4- IP assigned to Virtual NIC in the pod's network namespace.	**What you should know** 1- Facilitate forwarding within a cluster. 2- These differ from one scenario to the other	**What you should know** 1- How to assigned based on network requirement (Node, Pod, Services/Cluster IP) 2- Know subnet host count and restrictions 3- Node get IP from primary range, Pod and services from secondary range.	

Subnetting guide

Range	Guidance
Nodes	Node IPs are taken from the primary range of subnetwork associated with the cluster. Your cluster subnetwork must be large enough to fit the total number of nodes in your cluster. For example, if you plan to create a 900-node cluster, the subnet used with the cluster must be at least a /22 in size. A subnet size /22 contains $2^{(32-22)} = 2^{10} = 1024$ - 4 reserved IP addresses = 1020 IP addresses, which is sufficient for the 900 node IP addresses needed for the cluster.
Pods	Each node currently allocates a /24 ($2^{(32-24)} = 2^8 = 256$) block of Pod IP addresses. These Pod IP addresses are taken from the associated secondary range for Pods. The Pod range as determined by the `--cluster-ipv4-cidr` or `--cluster-secondary-range-name` flags must be at least large enough to fit (total number of nodes × 256) IP addresses. For example, for a 900-node cluster, you need 900 × 256 = 230,400 IP addresses. The IP addresses must come in /24-sized blocks, as that is the granularity assigned to a node. You need a secondary range of size /14 or larger. A /14 range of IP addresses results in $2^{(32-14)} = 2^{18} \approx 262k$ IP addresses.
Services	Every cluster needs to reserve a range of IP addresses for Kubernetes Service cluster IP addresses. The Service IP addresses are assigned from the associated secondary range for Services. You must ensure that the block of IP addresses is sufficient for the total number of Services that you anticipate to run in the cluster. You define the ranges defined using the `--services-ipv4-cidr` or `--services-secondary-range-name` flags. For example, for a cluster that runs at most 3000 Services, you need 3000 IP addresses to be used for cluster IP addresses. You need a secondary range of size /20 or larger. A /20 range of IP addresses results in $2^{(32-20)} = 2^{12} \approx 4k$ IP addresses.

Kubernetes networking example



Cloud DNS

What it is
Cloud DNS is a high-performance, resilient, global Domain Name System (DNS) service that publishes your domain names to the global DNS in a cost-effective way.

What you should know
1- Types Zones (managed, Public, Private, forwarding, peering)
2-Internal DNS, delegated subzones)

Key Points
1- On Prem connection
2- Private Zones
3- Importing Zone record-sets
4- Forwarding zones

Session Affinity

What it is
Session affinity sends all requests from the same client to the VM instance as long as the instance stays healthy and has capacity.

What you should know
1- Supported by the following LB (Internal, TCP and SSL proxy, HTTP(s) & Network)

Key Points
1- How each type of LB handle session affinity options (None, IP, Protocol, Port)

Logging

What it is
Log generation can be exported to Stackdriver Logging, Cloud Pub/Sub, Cloud Storage, or BigQuery.

What you should know
1- Benefit of logging
2 – What kinds of logs
3- How to view data

Key Points
1- General awareness of log types and viewing.

Flow logs

What it is
VPC Flow Logs record a sample of network flows sent from and to by VM instances. These are used for monitoring, forensics, real-time security analysis, and expense optimization.

What you should know
1- Cases to use this to gather info to lock down access, see traffic etc
2- How to enable

Key Points
1- What it records, how to read it

Route based VPN

What it is
Consider when the peer gateway cannot use BGP. In route based VPN, you specify only the remote traffic selector. Classic VPN **static routing.**

What you should know
1 - Local and remote traffic selector always **0.0.0.0/0**

Key Points
1- You must manually create and maintain the routes to the subnets in your VPC network on your peer routers.

Policy based routing

What it is
Consider when the peer gateway cannot use BGP. Policy based routing uses local and a remote traffic selectors. Use with classic VPN **static routing**

What you should know
1- Configurable remote and local traffic selectors

Key Points
1- You must manually create and maintain the routes to the subnets in your VPC network on your peer routers.

Review documents

DNS
Troubleshooting health
HTTPS logging
Network and Tunnel routing
Session affinity
Flow Logs
Import Record-sets
Static Routing

My experience

Routes based, Policy based, logging, DNS, session affinity these can be troublesome if you do not understand each concept clearly for exams. **Get my hint, really troublesome.**

Compute instance

What it is
Your virtual machine in the cloud. This is part of Google IaaS offering

What you should know
1- IP assignment internal, external
2- Static IP's

Key Points
1- Testing updates
2- **Tagging**

Key Management

What it is
By creating and managing SSH keys, you can allow users to access a Linux instance through third-party tools.

What you should know
1- **How to configure**
2- What are the risk

Key Points
1- How to assign to your VM's
2- How to remove from VM

DNSSEC

What it is
Prevents attackers from manipulating or poisoning the responses to DNS requests.

What you should know
1- How to set up
2- How to **disable**

Key Points
1- The components to make this work and be removed.

Cloud Armour

What it is
Google Cloud Armor security policies are made up of rules that allow or prohibit traffic from IP addresses or ranges defined in the rule.

What you should know
1- Where and how it works (Edge, HTTPS load balancing proxy)

Key Points
1- How it works (whitelist, blacklist)
2- DDOS

Cloud NAT

What it is
Allows virtual machine (VM) instances without external IP addresses and private (GKE) clusters to connect to the Internet.

What you should know
1- How it works

Key Points
1- Hide internal IP from external host.

IKEv1

What it is
IKEv1 limits remote traffic selectors to a single CIDR. Cloud VPN does not support creating a tunnel using IKEv1 with multiple Child SAs, each with a single CIDR

What you should know
1- Difference between **IKEv1** and **IKEv2**

Key Points
1- How this affect Multiple CIDR's traffic selectors Cloud VPN

Review documents

DNSSEC
Rolling Updates
URL_Map
NAT
Connecting using advanced methods

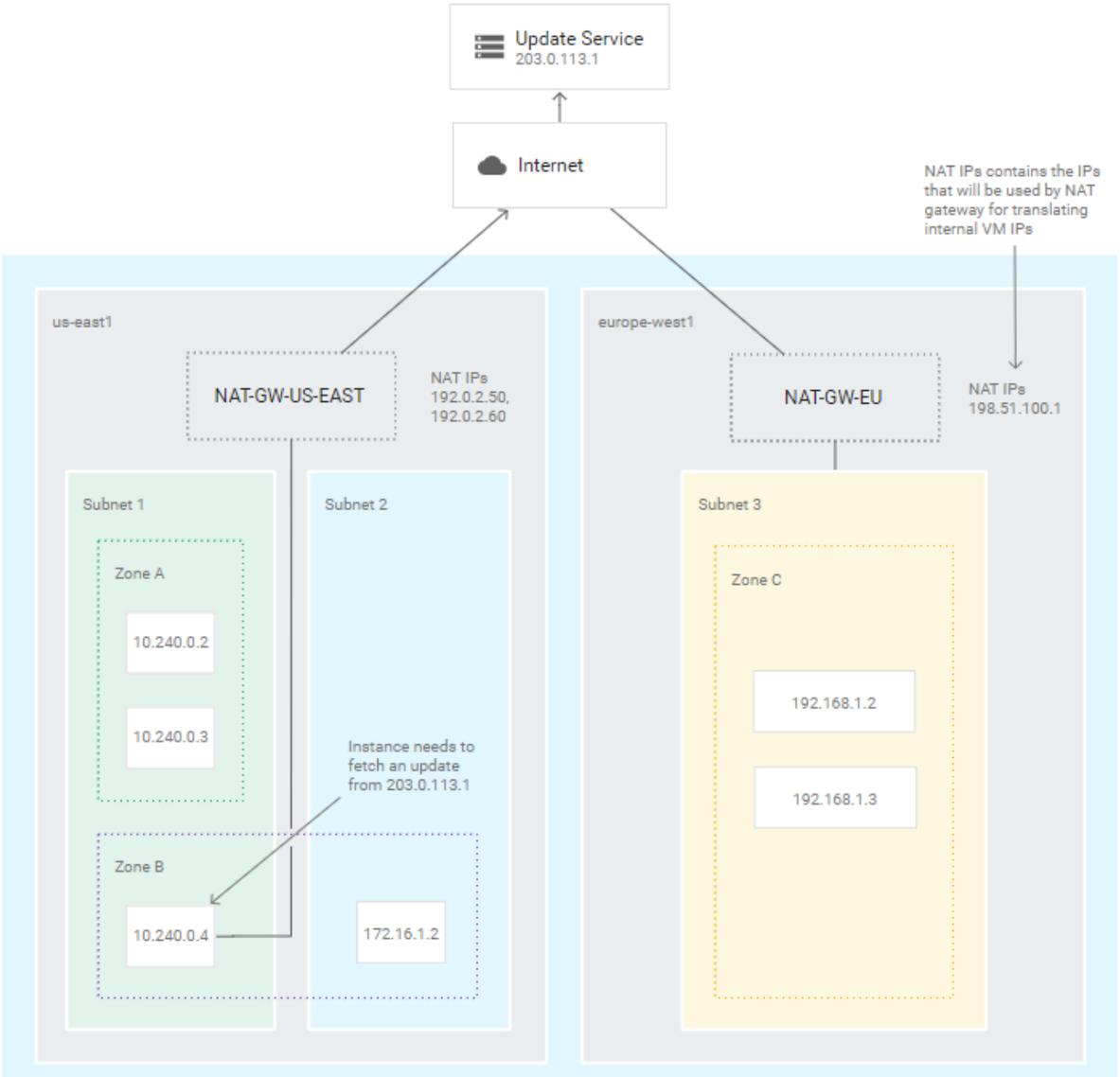
Video

DDoS

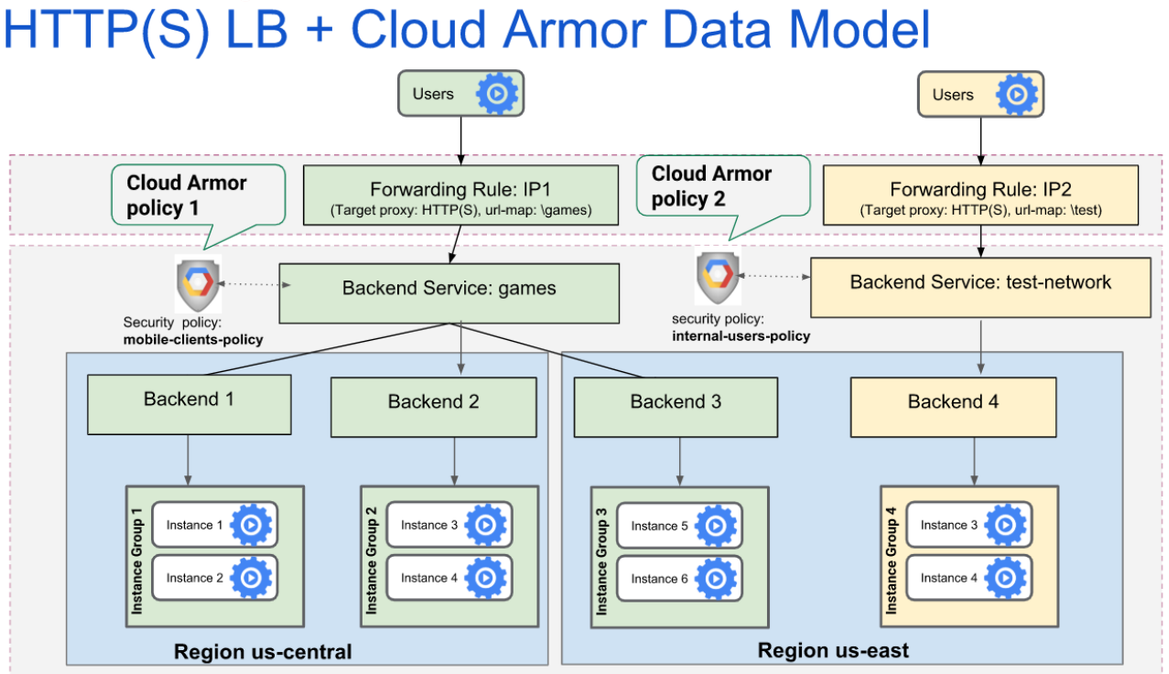
My experience

All these area combined made for some very challenging questions. It's worth spending a bit of time reviewing.

NAT image



Cloud Armour image



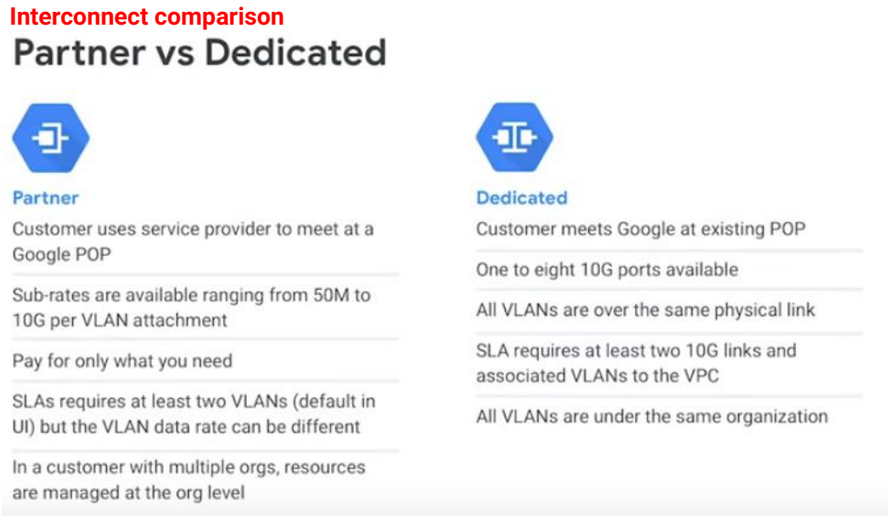
Session affinity image

Load balancer	Session affinity options
• Internal	• None • Client IP • Client IP and protocol • Client IP protocol and port
• TCP Proxy • SSL Proxy	• None • Client IP
• HTTP(S)	• None • Client IP • Generated cookie
• Network	Network Load Balancing doesn't use backend services. Instead, you set session affinity for network load balancers through target pools. See the `sessionAffinity` parameter in Target Pools.

VPC Sharing 	**What it is** Used to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs.	**Key points** 1- Centralised management 2- Firewall control 3- Internal RFC1918 communication	**What you should know** 1- When to use (depend of services and controls necessary etc) 2- Who gets billed	**Review documents** Hybrid Connectivity Shared VPC	**Video** CONNECTIVITY	**My experience** This will pop up. Who knows peering is sharing ☺. **Core topic**
VPC Peering 	**What it is** Access G Suite and Google Cloud features over VPN or the internet, while cutting egress fees. Connect directly with Direct Peering, or choose a partner with Carrier Peering.	**Key points** 1- When to peer 2- What services you have access to	**What you should know** 1- How to peer to a shared VPC	**Review documents** VPC Peering	Connecting to Datacentre	**My experience** This will come. Know requirements of peering and how to peer to shared networks. **Core topic**
VPN 	**What it is** Connect your on-premises or other public cloud networks to GCP Virtual Private Cloud (VPC) securely over the internet through IPSec VPN	**Key points** 1- How to setup 2- IPSEC used 3- Best practices	**What you should know** 1- Multiple tunnels 2- ECMP	**Review documents** Cloud VPN		**My experience** **Core area**. Make sure you know VPN very well. Know high availability, multi tunnelling various scenarios for use.
Dedicated Interconnect 	**What it is** Use dedicated Interconnect to connect to Google's network through a highly available, low latency connection. (10GB higher)	**Key points** 1- Single mode fiber 10GBase-LR 2- LACP for links & 802.1q Vlan 3- Support EBGP with multihop 4-Ipv4 link local addresses 5- Meet at Co Location facilities	**What you should know** 1- Type (system and custom) 2- Default route & Subnet route 3- Static and Dynamic routes 4- Min 10GB 5- Layer2	**Review documents** Dedicated Interconnect		**My experience** **Core area** well represented in exam. Did I say **well** represented?
Partner Connect 	**What it is** Use Google Cloud Interconnect - Partner (Partner Interconnect) to connect to Google through a supported service provider. (from 50 MB up)	**Key points** 1- Best case use 2- Min size 50MB 3- Not over the internet	**What you should know** 1- The IP Range used 2- How to assign static internal 3- How to change IP	**Review documents** Partner Interconnect		**My experience** **Core area** well represented in exam also. **If you don't know all the interconnect option well don't do the exam.**
VLAN 	**What it is** VLAN attachments (also known as **InterconnectAttachments**) determine which Virtual Private Cloud networks can reach your on-premises network through an interconnect	**Key points** 1- Works with Cloud router 2- Maximum speed 10 Gbps 3- Multiple VLANs	**What you should know** 1- Create VLAN attachments over Cloud Interconnect connections that have passed all tests and that are ready to use	**Review documents** Creating VLAN attachment		**My experience** Questions on this point may appears. You need a VLAN for what?
Dynamic routing 	**What it is** Dynamic routing is suitable for any size network. It frees you from maintaining static routes. Also, if a link fails, dynamic routing can automatically reroute traffic if possible.	**Key points** 1- Cloud router necessary 2- BGP session necessary	**What you should know** 1- IP automatically updated and propagated 2- Modes are Global or regional	**Review documents** Setting the network dynamic routing mode		**My experience** How are routes updated? Manually or automatically. Understand how this works.
Stackdriver 	**What it is** Stackdriver Logging allows you to store, search, analyze, monitor, and alert on log data and events from Google Cloud Platform and Amazon Web Services (AWS).	**Key points** 1- Individually enabled 2- Logging is supported for TCP and UDP only	**What you should know** 1- Troubleshooting viewing (Log entries missing, cannot view logs, where to apply logs)	**Review documents** Stackdriver	**Video** Stackdriver	**My experience** You should have an idea where to look, what rules are logged, priorities and how to fix.

Connection options

Interconnect comparison



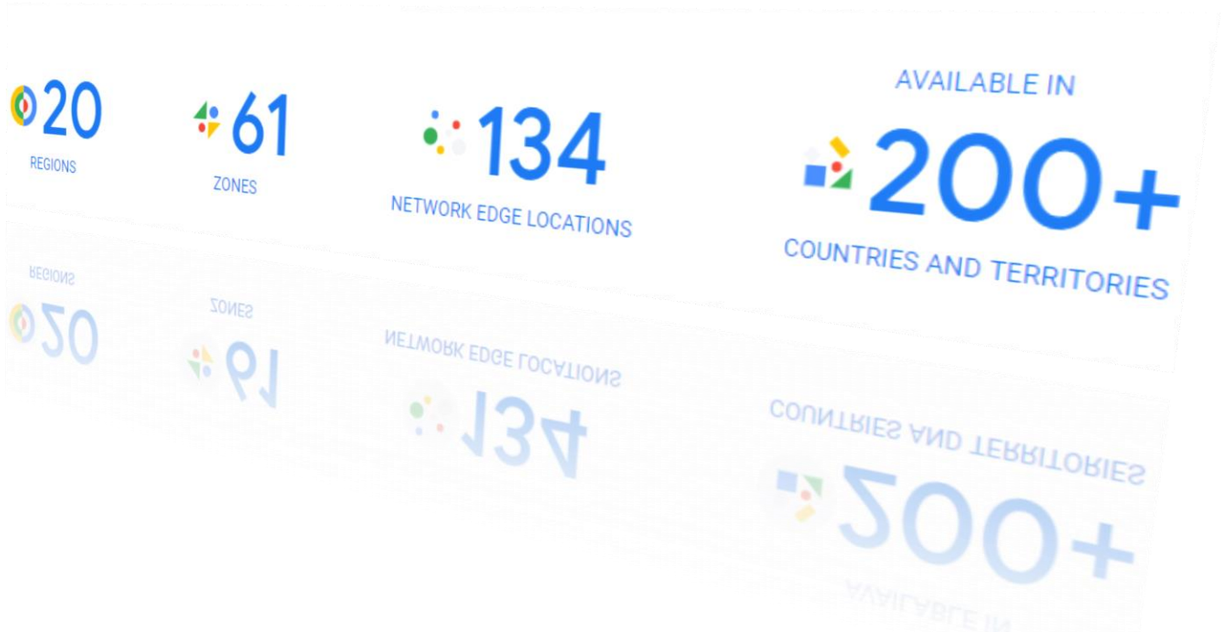
Cloud Networking

My closing thoughts

Networking is a core component of the cloud. In fact, public cloud is based on advanced SDN networking and the internet. Whether you are using code to deploy your environment or IaaS, the end result is that you want people to connect to your apps and services. If your apps are not reachable then it makes no sense. Constructing a well-defined network is important to ensure content delivery and performance is kept at it's **SLO** ☺ as much as possible.

Video
A year in GCP networking

Google presence



Thanks for reviewing

Please visit the official certification outline HERE

Official practice test HERE

ps. These are my notes and tips that helped me pass the networking exam on the second attempt this is a tough exam. Every area on the document represents a topic that has a strong probability of appearing. Google may change the exam requirements at any time so always review the outline.

The knowledge is free it just cost me some time to put together. Please share with your network who may be interested in GCP Networking or need a quick refresher on networking topics.

You can also check my other Google **prep notes** for the **Security, DevOps and Engineer** exam HERE

Bonne Journée