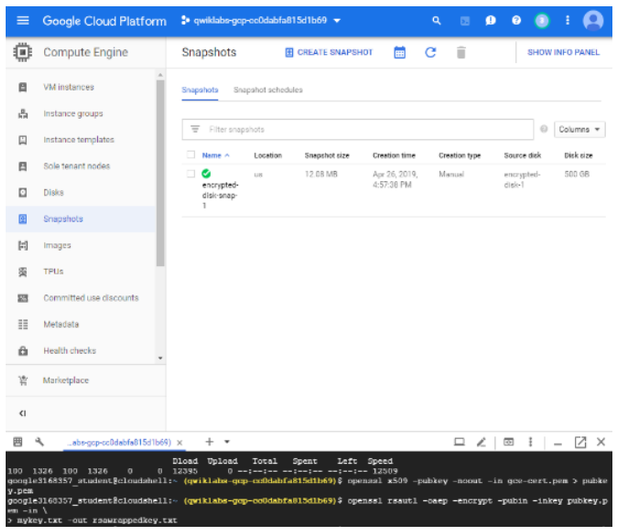
Start Cloud Now

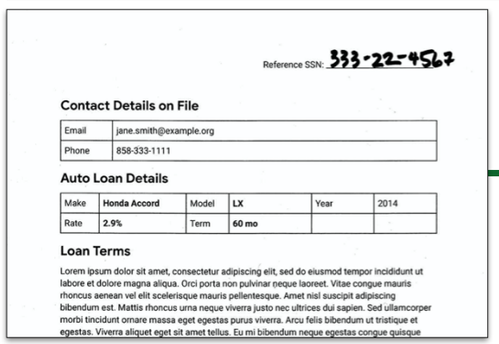
Google Cloud Professional Cloud Security Engineer Exam

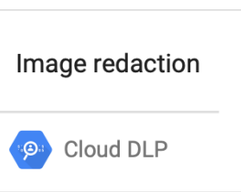
Prep Notes by

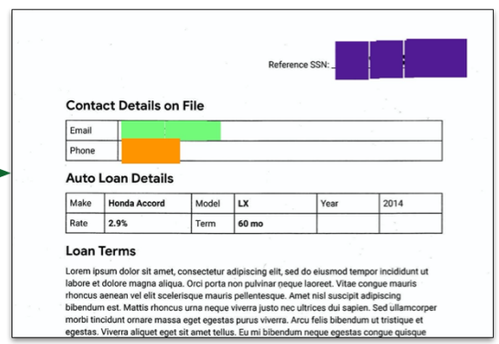
Ammett

V2



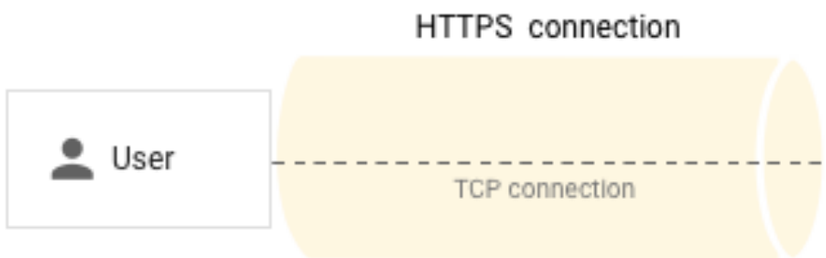


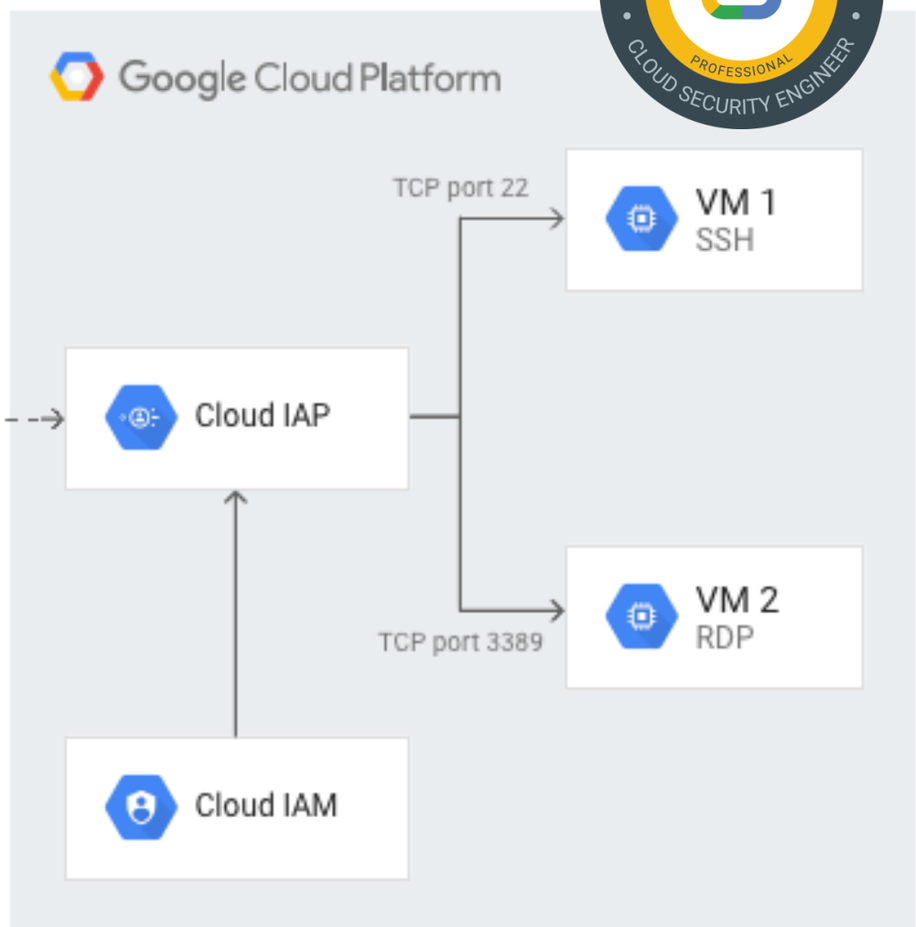




1

2





https://t.me/learningnets

By Ammett:

Google Cloud Professional Cloud Security Engineer

Exam Prep Sheet by Ammett

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

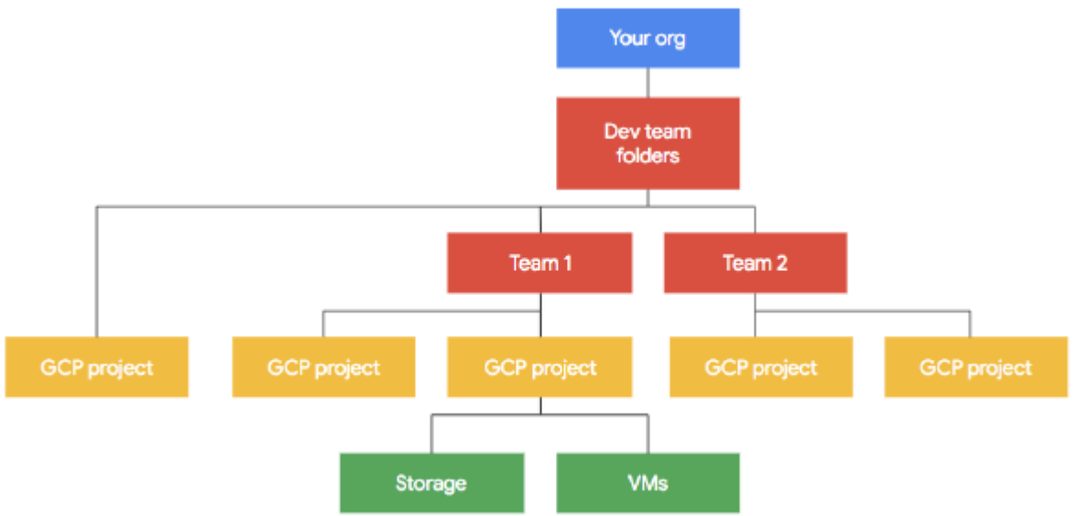
V2.1: 05-2021

White papers you must review

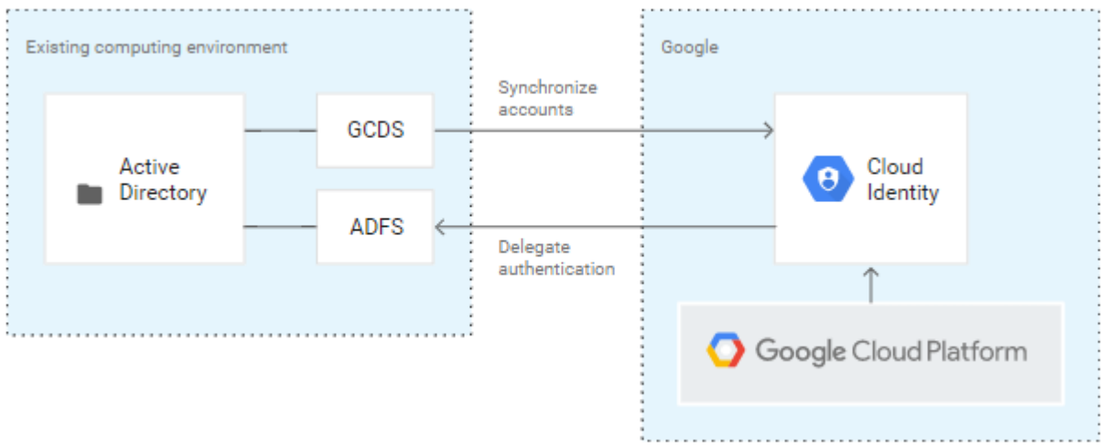
1 - 7-best-practices-for-building-containers
2 - Best practices for enterprise organizations
3 - Choosing a Load Balancer
4 - Cloud Audit Logs
5 - Cloud IAP for on-premises apps
6 - DNS Security (DNSSEC)
7 - Envelope encryption
8 - Federating Google Cloud Platform with AD
9 - Firewall Rules Overview _ VPC
10 - Forseti Security
11 - Key rotation _ Cloud KMS
12 - PCI_DSS_Shared_Responsibility_GCP
13 - Retention policies using Bucket Lock
14 - Scenarios for Exporting Logging Data
15 - Logging Secret management with Cloud KMS
16 - Securing your app with signed headers
17- DLP

Organisation Structures	**What it is** GCP 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.	**What you should know** 1- Flow (Organisation, Folders, projects, resources) 2- Where to manage permissions for groups, department, entire organisation, etc 3- Permissions level necessary	**Review documents** **Resource Hierarchy** **Organization Policy Service**	**Video** **Google Cloud Platform resource hierarchy** **GCP resource Organisation and Access management**	**My experience** This area is fundamental however you really need to understand how to control to get the separation, how it should be designed and restrictions applied.
Cloud Identity	**What it is** A unified identity, access, app, and device management (IAM/EMM) platform. (similar to Microsoft AD)	**What you should know** 1- Federations 2- AD integrations / Hybrid LDAP 3- Saml 2.0 & OpenID 4- Single Sign On 5-Service accounts	**Review documents** **Cloud Identity** **Authenticating corporate users in a hybrid environment** **Federating Google Cloud with Active Directory**	**Video** **Identity and authorization** **Exploring Cloud Identity**	**My experience** This is a core area in the exam. You should know the various scenarios and how integrations work.

Organisation Structure - diagram



Federating Active Directory with Cloud Identity-diagram



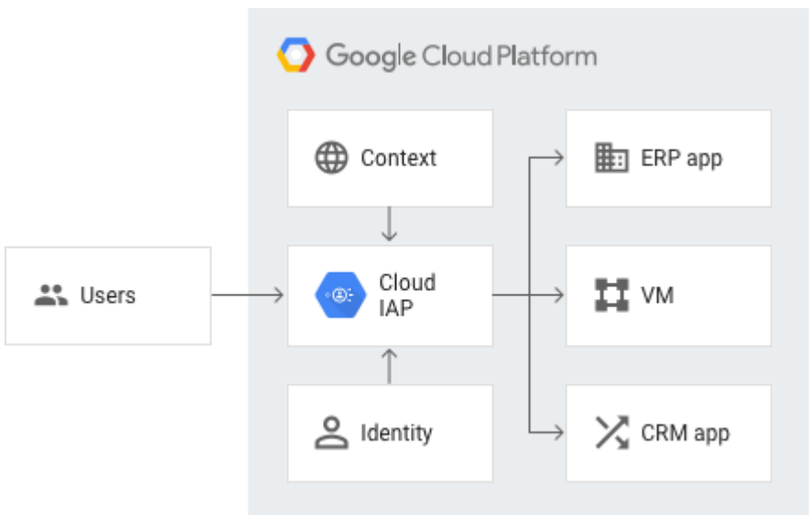
https://t.me/learningnets

Start Cloud Now

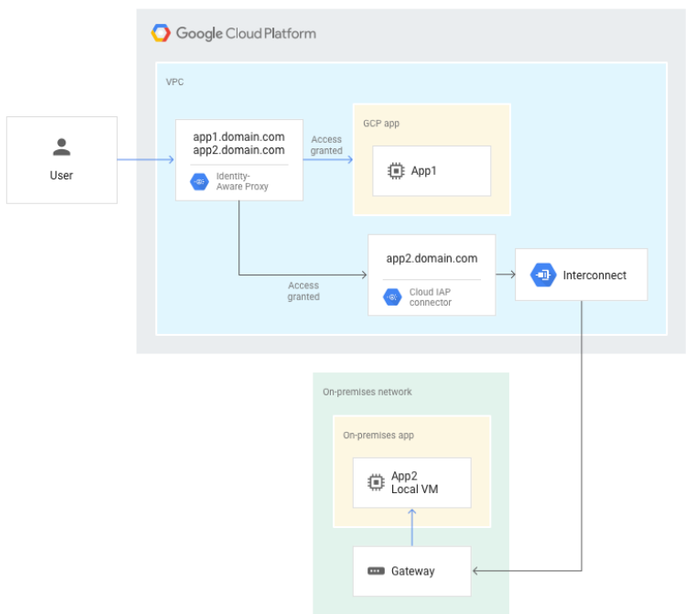
By *Ammett:*

Cloud IAM	**What it is** Cloud IAM which lets you manage access control by defining *who* (identity) has *what access* (role) for *which* resource.	**What you should know** 1- Best way to manage (use groups) 2- MFA Multiple factor authentication. 3- Roles (primitive, predefined & custom) 4- Roles necessary to do certain functions 6- Password min requirements	Review documents How IAM works Cryptographic Second Factors Create a strong password Modern password security Roles	Video Better Practices for Cloud IAM	**Labs** Cloud IAM: Qwik Start Custom Roles Service Account Roles	**My experience** This wasn't too bad however if you don't know it gets confusing and leads to misinterpretation of questions
Identity Aware Proxy	**What it is** Cloud Identity-Aware Proxy (Cloud IAP) controls access to your cloud applications and VMs running on (GCP)	**What you should know** 1- How it works (HTTPS) 2- JWT (signed headers) 3- How to configure 4- On prem flow 5- TCP forwarding	Review documents Identity-Aware Proxy overview Securing your app with signed headers IAP for on-premises apps	Video Identity Aware Proxy Beyond Corp	**Labs** User authentication with Identity-Aware Proxy	**My experience** Understanding the flow is important and where and when to use it. That made the difference in selecting the correct answer if it wasn't obvious
Google security model	**What it is** Google's end to end security process built up over 15+ year to secure their various offering including Google Cloud Platform	**What you should know** 1- Shared responsibilities on various service types (PaaS, IaaS, SaaS) 2- Compliance (ISO 27001 etc, PCI) 3- Default security google applies 4- Encryption on by default 5- Data removal, hardware handling	Review documents Trust and Security Google security whitepaper PCI DSS shared security model	Video Google Cloud Security Shared Responsibility: What This Means for You as a CISO		**My experience** A few of these types came up not much but I can tell you these can easily cost you a mark or 3 if you are not familiar at a reasonable level. Be familiar with 27001, 27017, 27018, PCI.

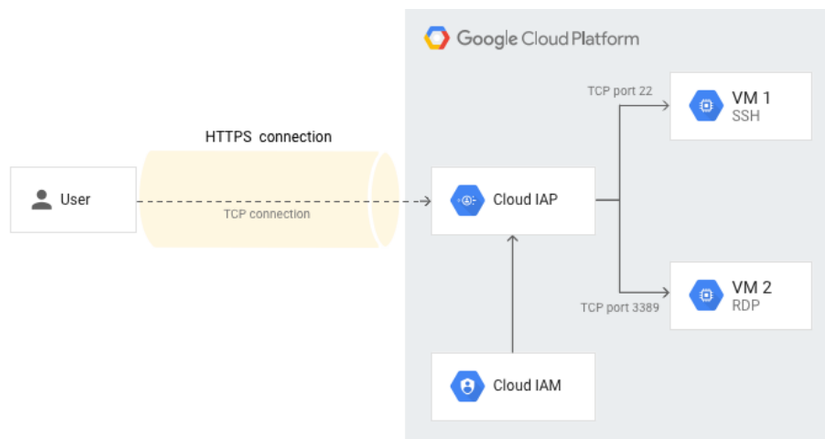
Cloud IAP flows - diagram



On Prem flow - diagram



TCP forwarding-diagram



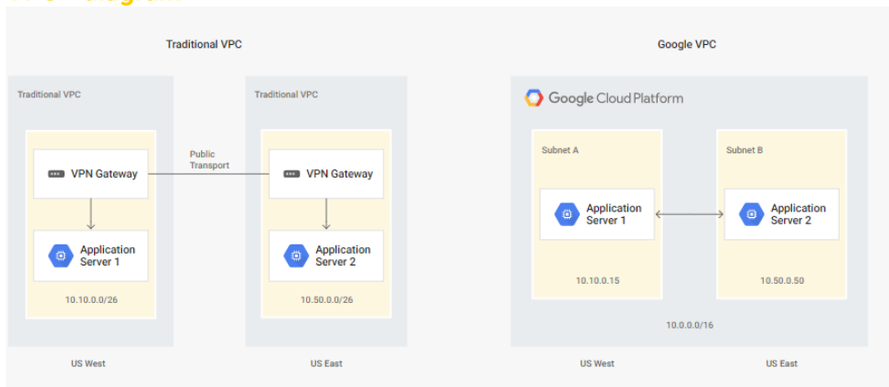
https://t.me/learningnets

Start Cloud Now

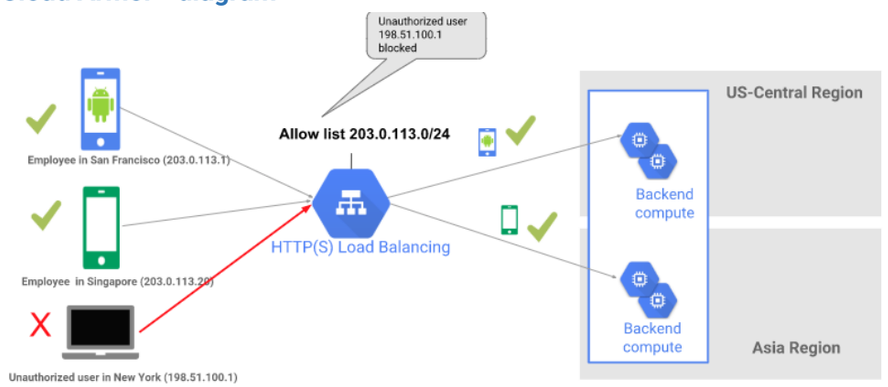
By *Ammett:*

VPC	**What it is** A VPC network, is your virtual network in the cloud just like an on prem physical network or data center or office network.	**What you should know** 1- Default network, How to design your own custom VPC for your production projects 2- How to get traffic flowing 3- RFC1918 4- Internal and external access	Review documents **VPC network overview** **VPC service control**	Video **VPC's** **Securing Data with VPC service control**	**Labs** **Multiple VPC networks**	**My experience** Can't have security without networking understand very well. Well featured in the exam
Firewall	**What it is** Allow or deny traffic to and from your virtual machine (VM) etc, based on a configurations you specify.	**What you should know** 1- How they work (Stateful) & Scope 2- Implied rules 3- Default rules 4- Effect of sharing, peering, etc 5- Filtering methods (IP, Tags, SA)	Review documents **Implied rules** **Filtering by service accounts**	Video **Firewalls rules**	**Labs** **VPC Networks - Controlling Access**	**My experience** There are some implied and default rule know these. Also, how to define your rules (source, dest, pot, protocol, action, priority)
Cloud Armor	**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 it works (Edge, HTTPS load balancing proxy) 2- How works (whitelist, blacklist, IAP, etc) 3- Restrictions Cloud armour and CDN	Review documents **Cloud Armor Security policy**	Video **Journey with Cloud Armor**	**Labs** **HTTP Load Balancer with Cloud Armor**	**My experience** Goes well with security and securing apps and load balancers.
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 etc 2- What it records, how to read it 3- How to enable	Must review documents **Using VPC Flow Logs**	Video **GCP Network and Security**	**Labs** **VPC Flow Logs - Analyzing Network Traffic**	**My experience** Another one of the areas where a question or two came up and can easily gain you a much-needed mark.

VPC - diagram



Cloud Armor - diagram



https://t.me/learningnets

Start Cloud Now

By *Ammett:*

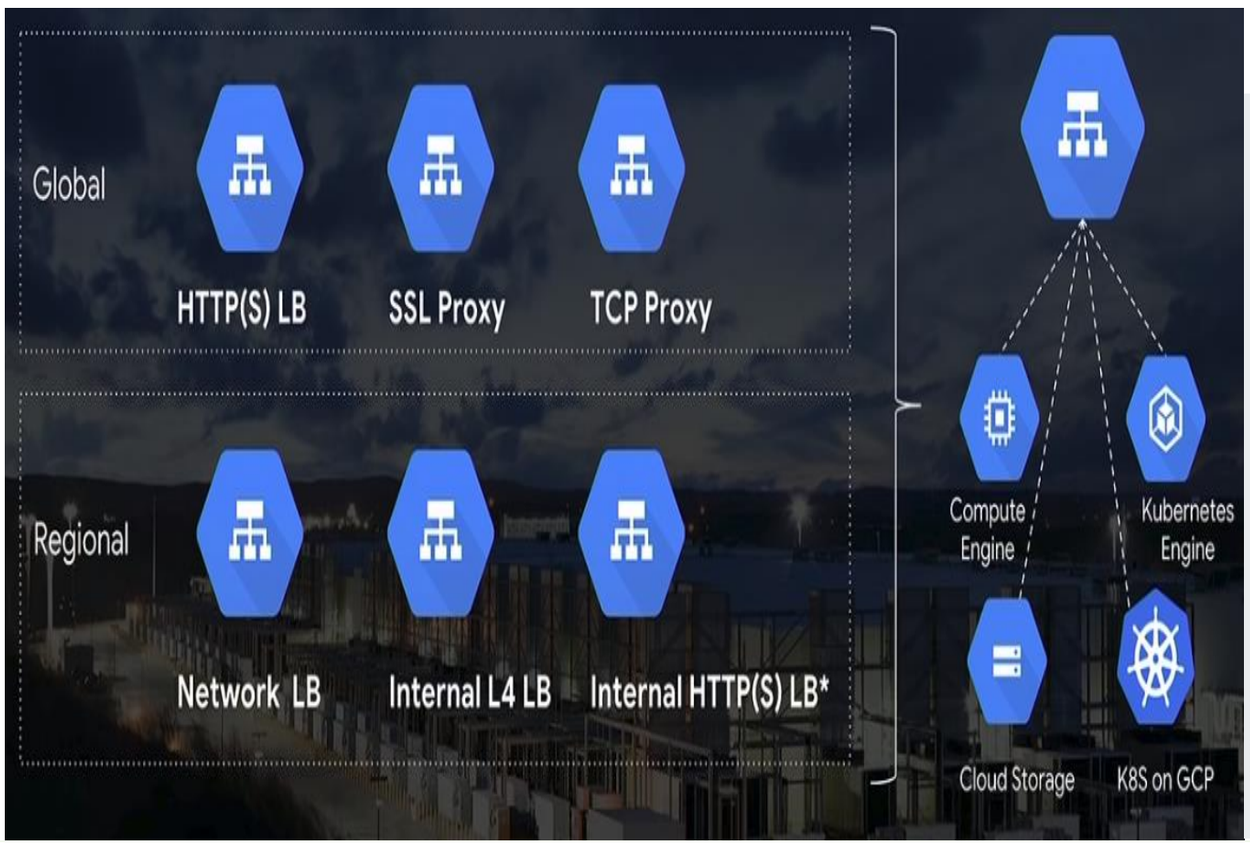
HTTP(S) Load balancer	SSL Proxy	TCP Proxy	Network Load balancer	Internal load balancer
What it is Load balancer for HTTP(S) traffic, global, external, 80 or 8080 on 443	**What it is** Load balancer for TCP with SSL offload, global, external. (25, 43, 110, 143,195, 443, 465, 587, 700, 993, 995, 1883, 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 you should know 1- Scope global 2-HTTPS traffic	**What you should know** 1- Scope Global 2- Non HTTPS traffic SSL termination	**What you should know** 1- Global 2 – TCP/UDP traffic	**What you should know** 1- Scope regional 2- TCP/UDP traffic	**What you should know** 1- Scope Regional 2 - Internal TCP/UDP traffic

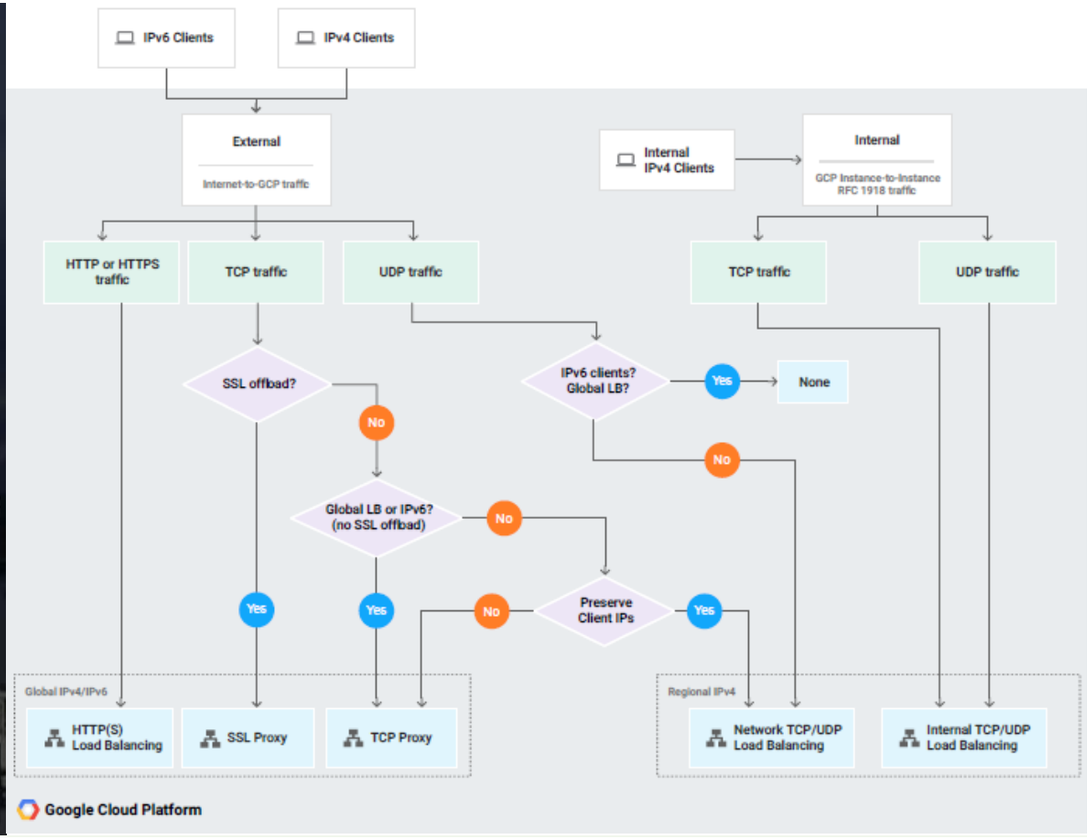
Review documents

Choosing a load balancer

Video
Cloud Load balancers

My experience
This is tricky so know the main points (Global vs Regional, External vs Internal, Traffic type)





https://t.me/learningnets

Start Cloud Now

By *Ammett:*

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.

What you should know
1- Centralised management
2- Firewall control
3 – internal RFC1918

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.

What you should know
1- When to peer what
2 - services you have access to

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

What you should know
1- Over internet
2 – IPSEC used
3 – dynamic SETUP

Dedicated Interconnect

What it is
Use dedicated Interconnect to connect to Google's network through a highly available, low latency connection. (10GB higher)

What you should know
1- Reason to use this
2- Min 10GB
3 – Not over the internet

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)

What you should know
1- Best case use
2 – Min size 50MB
3 – not over the internet

Review documents
- **Hybrid connectivity options**
- **Shared VPC overview**

Video
CONNECTIVITY

My experience
The perfect question area to test if a person knows how each of these really work. I mean all connections are not the same, or are they?

DNS SEC

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

What you should know
1- What it protects

Private Access

What it is
Allows VM instances with internal (**RFC 1918**) IP addresses to reach certain APIs and services without internet access.

What you should know
1- How to enable (this is important)

Cloud NAT

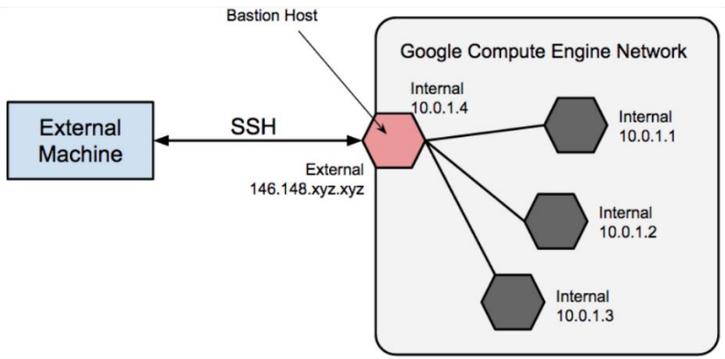
What it is
Google Cloud Platform (GCP) virtual machine (VM) instances without external IP addresses and private (GKE) clusters to connect to the Internet.

What you should know
1. How it works

Bastion Host

What it is
Bastion hosts provide an external facing point of entry into a network containing private network instances from the Internet

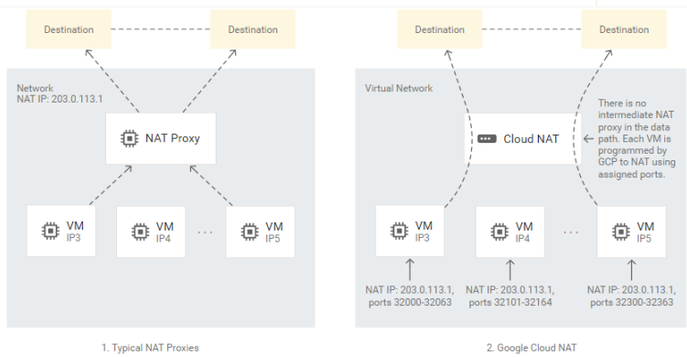
What you should know
1- Where it sits



CIDR Subnets

What it is
You can choose any private RFC 1918 CIDR block for the primary IP address range of the subnet.

What you should know
1- Overlapping ranges,
2 – Subnet Mask based on required host
3- Reserved IP addresses



Review documents
- **DNSSEC**
- **Cloud NAT**
- **Private Access**

Labs
Config private access and cloud NAT

My experience
Some of these may pop up if not all so just know these and they are pretty straight forward.

https://t.me/learningnets

Start Cloud Now

By *Ammett:*

Cloud KMS

What it is

Cloud KMS is a cloud-hosted key management service that lets you manage encryption for your cloud services the same way you do on-premises. You can generate, use, rotate, and destroy cryptographic keys.

What you should know

1- It's purpose
2- What are the cases you should use it.

CMEK

What it is

For greater control you can use customer-managed encryption keys (CMEK). This way you control and manage key encryption keys in Cloud KMS

What you should know

1- What products support this service (BigQuery, Cloud Build, Cloud Dataproc, Cloud Storage, Compute Engine)
2 – Know the step

CSEK

What it is

If you supply your own encryption keys, Google uses your key to protect the Google-generated keys used to encrypt and decrypt your data

What you should know

1- Supported by Compute and Cloud storage
2 – This key replaces the KEK
3 – Know the step (very important)

Key rotation

What it is

In Cloud KMS, a *key rotation* is represented by generating a new key version of a key, and marking that version as the *primary* version.

What you should know

1- Reason to rotate keys
2- Method automatic or manual, regular, irregular
3 – Commands

Managing secrets

What it is

Applications often require access to small pieces of sensitive data at build or run time. These pieces of data are often referred to as *secrets*.

What you should know

1- Choosing a secret management solution
2 – Rotating secrets

Review documents

- Customer supplied encryption keys (CMEK)
- Envelop encryption
- Key rotation
- Secret management

Video - **KEYS**

Labs

- Encrypt and decrypt data with Cloud KMS
- Encrypt and decrypt Cloud KMS Asymmetric
- Sign and verify data with Cloud KMS

My experience

Key management, encryption stuff is super important. I think one of the more featured areas of the exam. You will get questions on this. Know all situations, a bit on HSM, and which key type is used & most importantly, which products support which type. Know like the alphabet.

Cloud Security Scanner

What it is

The Cloud (Web)Security Scanner identifies security vulnerabilities in your App Engine, Compute Engine and Google Kubernetes Engine web applications.
It can automatically scan and detect four common vulnerabilities, including cross-site-scripting (XSS), Flash injection, mixed content (HTTP in HTTPS), and outdated/insecure libraries.

What you should know

1- Use cases scanning

Forseti

What it is

If you want to monitor your GCP resources to ensure that access controls are set as intended, this will allow creating rule-based Policies to codify your security stance.

What you should know

1- How to enable (this is important)

Kubernetes

What it is

The Kubernetes networking model relies heavily on IP addresses. Services, Pods, Containers, and nodes communicate using IP addresses and ports.

What you should know

1- How it works
2- Containers and pods
3- How to secure
4- Updating

DLP

What it is

With the Cloud DLP, you can easily classify and redact sensitive data contained in text-based content and images, including content stored in Google Cloud Platform storage repositories.

What you should know

1-How it works (Redact, Crypto-based, Masking, etc)
2 - How to configure and regex

G Suite

What it is

Google's SaaS offering comprised of Gmail, Docs, Drive, Calendar, Meet and more for business.

What you should know

1-High level administration
2 - Managing users, setting up domain, IAM, Super user account.

Review documents

- Web Security Scanner
- Forseti
- 7 best practices for building containers
- Kubernetes
- DLP
- REGEX
- Transformation

Video:
DLP
KUBERNETES

My experience

Forseti, CSS, Kubernetes and DLP are topic that you should know especially DLP which is super cool. You will get questions on these.

https://t.me/learningnets

Start Cloud Now

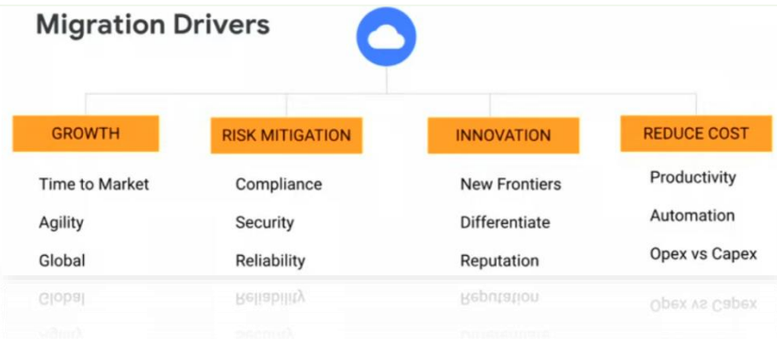
By *Ammett:*

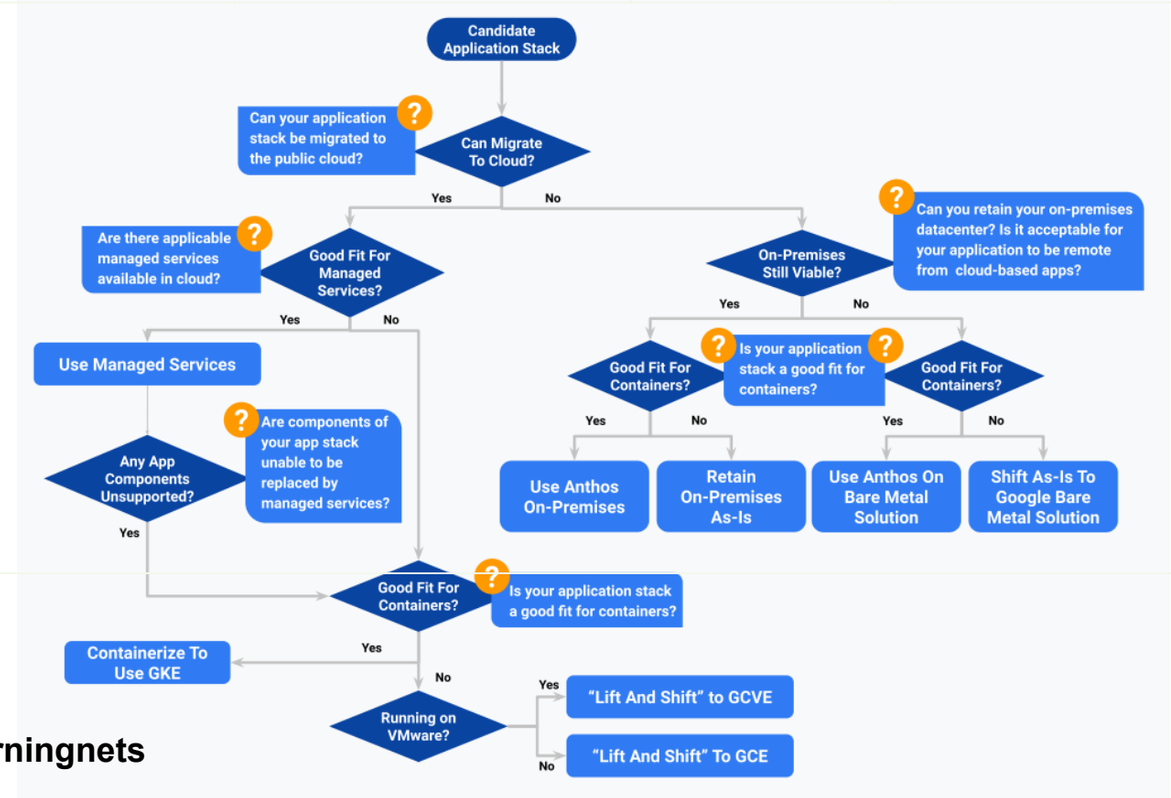
BigQuery	Cloud Storage	Compute Engine	Google Cloud's operations suite (formerly Stackdriver)	SIEM	
What it is BigQuery is a serverless, highly-scalable, and cost-effective cloud enterprise data warehouse that enables super-fast SQL queries using the processing power of Google's infrastructure.	**What it is** Unified object storage for developers and enterprises	**What it is** Google Compute Engine delivers virtual machines running in Google's innovative data centers and worldwide fibre network	**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).	**What it is** Security Information and Event Management (SIEM) software has a variety of uses. GCP has integration to these and many others	**Review documents** ▪ **Design patterns for exporting logging data** ▪ **Scenarios for exporting Cloud Logging data** ▪ **4 steps for hardening your Cloud Storage buckets** ▪ **Retention policies and retention policy locks** **Video** **CLOUD STORAGE** **Exporting** **BIGQUERY** **My experience** You can't have security without audit, storage and logging. These areas will come in one form or the other be familiar with and integrations also.
What you should know 1- Authorised views 2- How to export data 3 – Cloud DLP	**What you should know** 1-Types (nearline, coldline) Object storage. 2- Encryption options (default, CSEK, CMEK) 3- How to retain Data 4- Migrate Data	**What you should know** 1- Secured images 2- How to secure access 3- How to update	**What you should know** 1- Used for compliance 2- Used for security analytics 3- Used for SIEM	**What you should know** 1- How you would set up integrations	
Super User accounts	DDoS	Dataproc	App Engine	Cloud Audit logs	
What it is To configure your Google Cloud Platform (GCP) Organization resource, you need to use a G Suite or Cloud Identity super admin account.	**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** Cloud Dataproc is a fast, easy-to-use, fully managed cloud service for running **Apache Spark and Apache Hadoop** clusters	**What it is** Build and deploy applications on a fully managed platform. Scale your applications seamlessly from zero to planet scale without having to worry about managing the underlying infrastructure.	**What it is** Cloud Audit Logs are a collection of logs provided by Google Cloud Platform that provide insight into operational concerns related to your use of Google Cloud services	**Review documents** ▪ **DNS Security Extensions (DNSSEC)** ▪ **DDoS** ▪ **AppEngine** **Video** **DDoS** **AUDIT LOGS** **My experience** Be familiar with types of access certain accounts have, deployment methods, types of audit logs you may need. These will be featured
What you should know 1- What they are used for 2- Recommended limits	**What you should know** 1- How to prevent with GCP tools	**What you should know** 1. How it works, what it is used for	**What you should know** 1- Discovers vulnerabilities 2- Shared responsibility of service	**What you should know** 1- Data access 2- System 3- Admin	

https://t.me/learningnets

Start Cloud Now

By *Ammett:*

IaaS	**What it is** Think Datacenter (compute, storage, networking).	**What you should know** 1- Shared responsibility for these and what they are	Review documents **About Google Services**	**Click to see large version** 	**My experience** Understand the shared responsibility model and the basics also. These can be tricky if you don't know them.
PaaS	**What it is** Think code provisioning without infrastructure hassle	**What you should know** 1- Shared responsibility for these and what they are	Review documents **About Google Services**		
Migrations	**What it is** From legacy apps to cloud, from on prem to cloud.	**What you should know** 1- Set up in cloud 2- Secure in cloud 3- Network in the cloud	Review documents **Migration to Google Cloud** **Guide to application migration**	**Video** **Modernizing and Migrating to Cloud**	



Thanks for reviewing

Please visit the official certification outline HERE

Practice test HERE

ps. These are my notes and tips that helped me pass the exam on the second attempt. I kept them light and not too comprehensive. The actual exam requirements may change as technology evolves so please review Google's outline.

The sheet is free it just cost me some time to put together. So please share with your network who may be interested in GCP security. If it helps give me a shoutout on LinkedIn.

Check out all my Google prep sheets for the Network, DevOps and others **HERE**

Bonne Journée

https://t.me/learningnets

By *Ammett:*