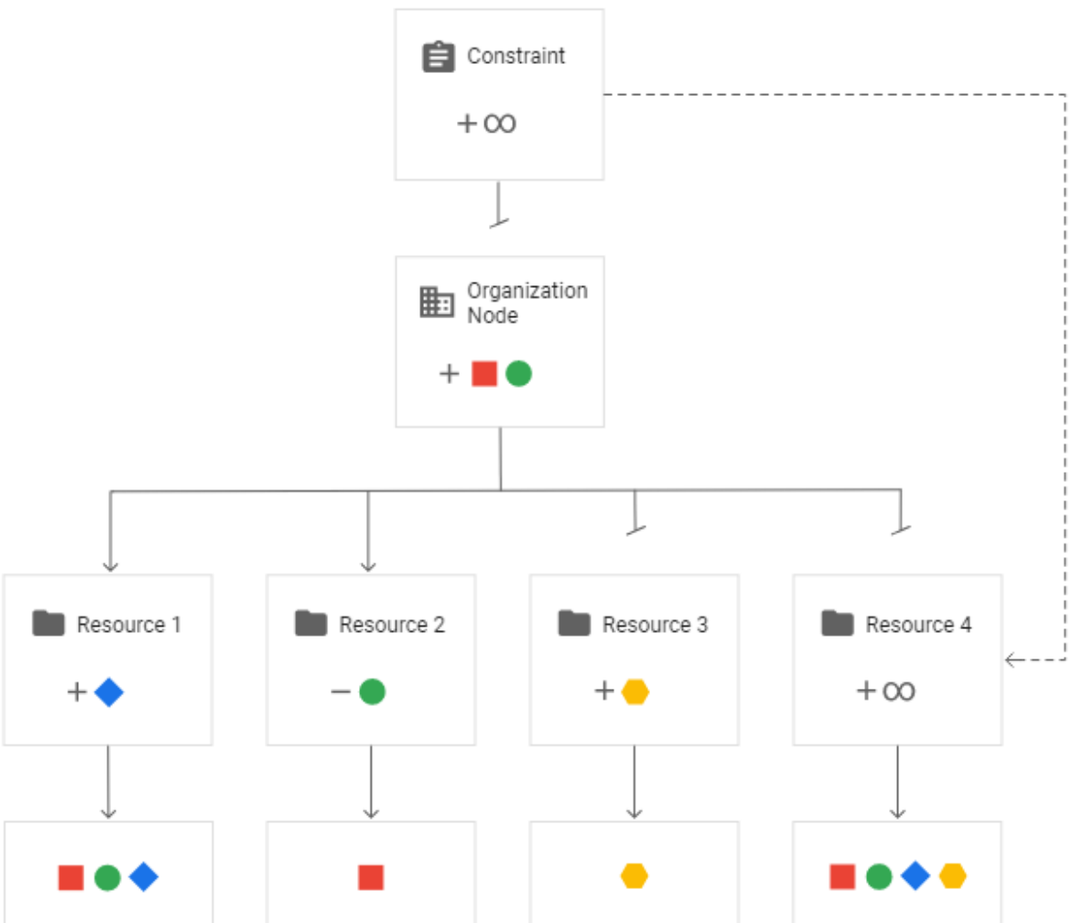
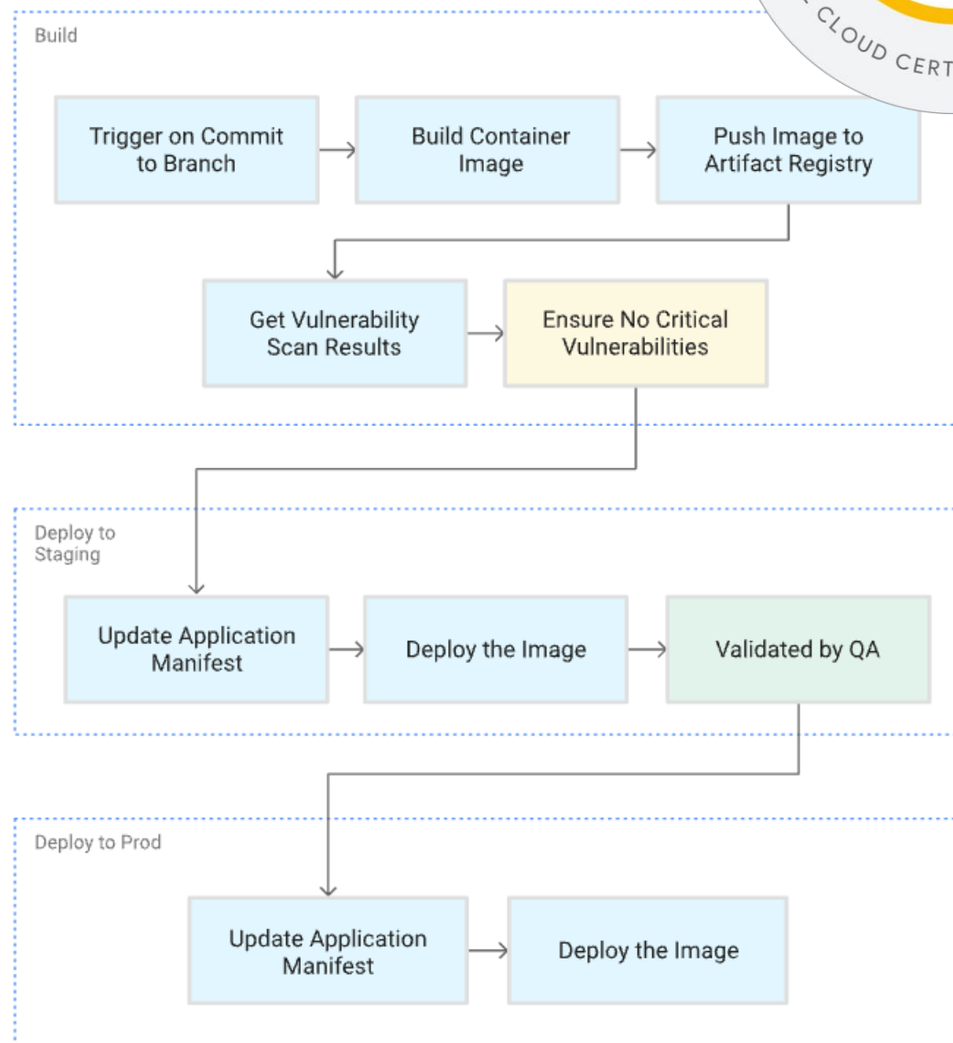
Start Cloud Now

Google Cloud Professional Cloud Security Engineer Exam

Prep Notes by

Ammett v4





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.

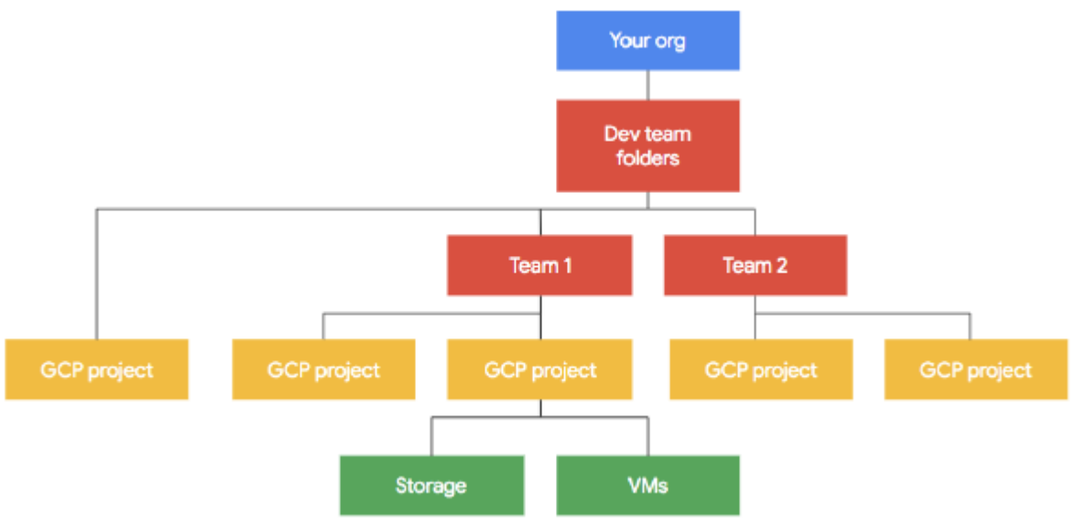
V4: 02-2024

White papers you must review

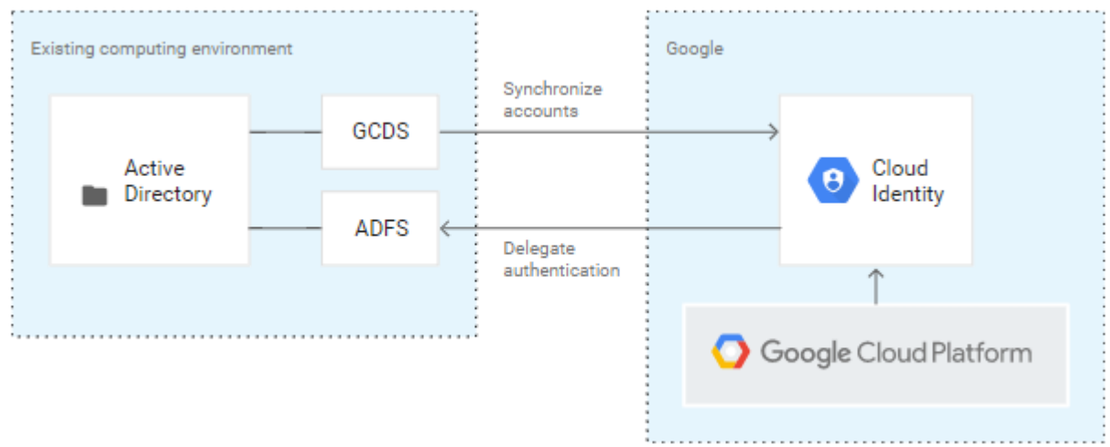
1 - 7-best-practices-for-building-containers
2 - Best practices for enterprise organizations
3 - Choosing a Load Balancer
4 - Cloud Audit Logs
5 - Cloud IAP for on-premises apps
6 - DNS Security (DNSSEC)
7 - Envelope encryption
8 - Federating Google Cloud Platform with AD
9 - Firewall Rules Overview _ VPC
10 - Pseudonymization
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 - DLP
17- Google Cloud security foundation guide

	What it is	What you should know	Review documents	Video	My experience
Organisation Structures	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.	1- Flow (Organisation, Folders, projects, resources) 2- Where to manage permissions for groups, department, entire organisation, etc 3- Permissions level necessary	**Resource Hierarchy**	**Google Cloud Platform resource hierarchy**	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. Understand constraints.
Cloud Identity	A unified identity, access, app, and device management (IAM/EMM) platform. (similar to Microsoft AD)	1- Federations 2- AD integrations / Hybrid LDAP 3- SAML 2.0 & OpenID 4- Set up SSO 5- Service accounts 6- Cloud Directory Sync 7- Groups control workspace admin	**-Cloud Identity** **-Authenticating corporate users in a hybrid environment** **-Federating Google Cloud with Active Directory** **-Workload Identity Pool & Service account impersonation**	**Identity and authorization** **Exploring Cloud Identity**	Spend some time to understand well how you integrate and also manager the account and security. How Two factor authentication may come into effect. Super user account. A tricky bunch of question my come on this topic.

Organisation Structure - diagram

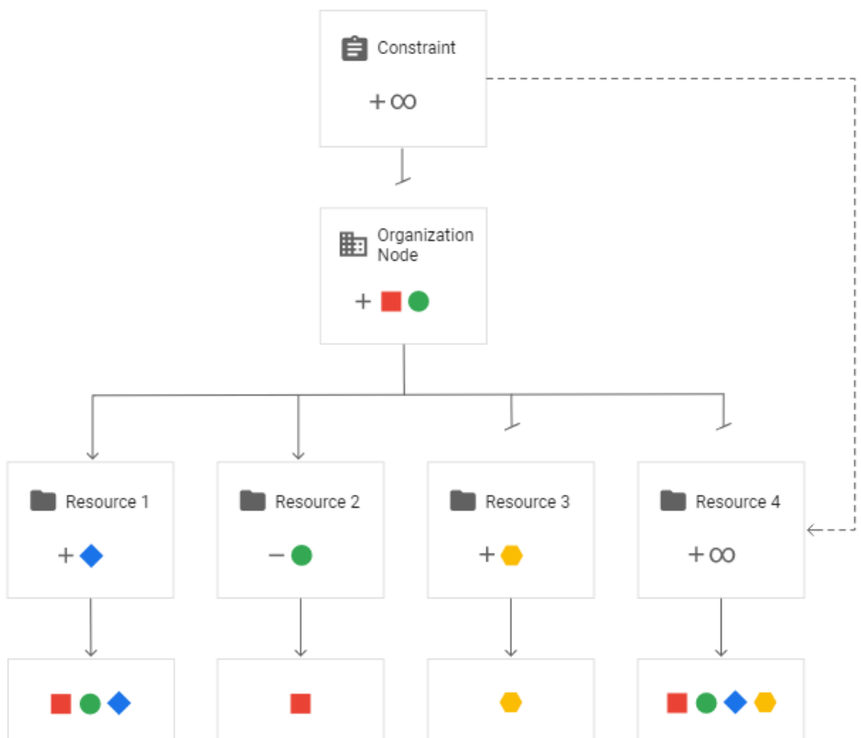


Federating Active Directory with Cloud Identity-diagram

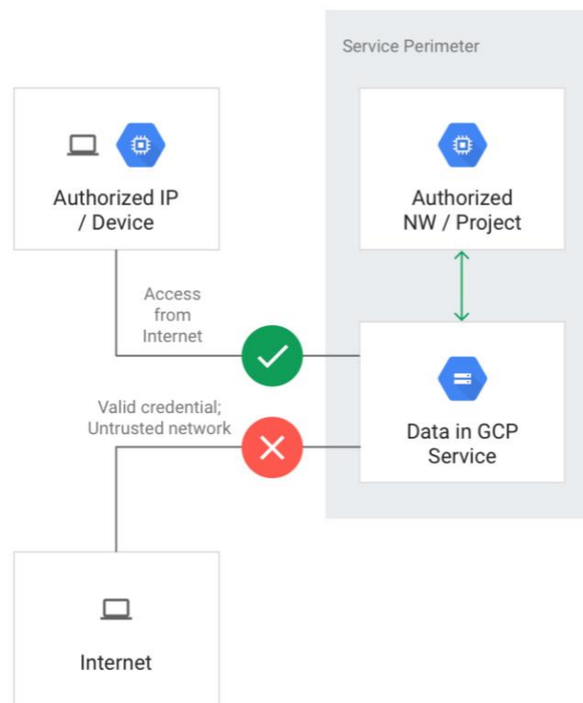


	What it is	What you should know	Review documents	Video	My experience
Organization policies	The Organization Policy Service gives you centralized and programmatic control over your organization's cloud resources	1- How to restrict access 2- Which level to apply constraints at 3- Permissions level necessary 4 – How list at higher level affect other level 5 – review list of constraints `constraints/compute.restrictXpnProjectLienRemoval`	**Organization policy Service** **Organisation policy resource Hierarchy** **Resource constraints** **Restricting Resource locations** **Restricting domain**	**GCP resource Organisation and Access management** **What is Google Cloud's Organization Policy Service**	Understand constraints you may come across various types of constraints.
VPC service controls	VPC Service Controls lets you mitigate data exfiltration risks by isolating resources of multi-tenant Google Cloud services.	1- How it work 2- How to allow access (ingress and egress) 3- How to prevent data exfiltration 4-Enforced and dry run mode	**VPC service control** **VPC service perimeter bridges** **VPC ingress and egress** **Dry Run mode**	**VPC service controls**	Important topics to control security in your VPC.

Organization policy

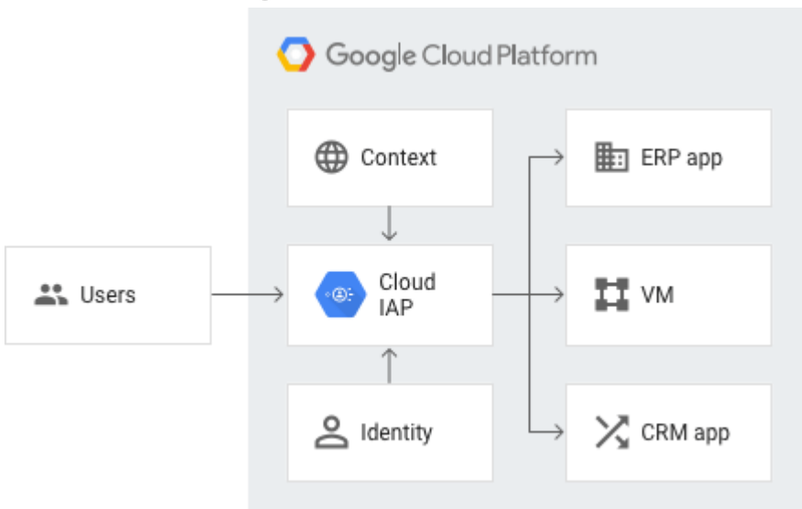


VPC-SC

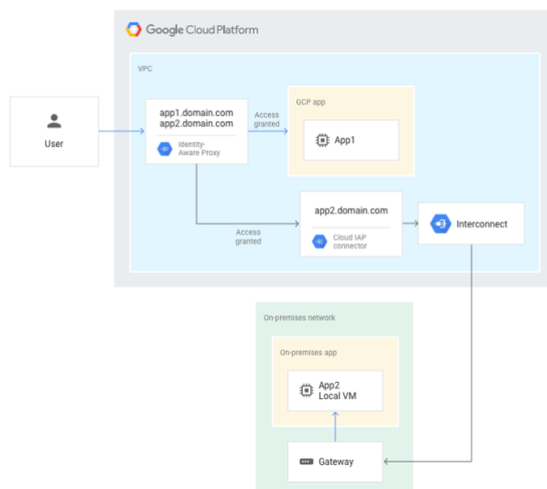


	What it is	What you should know	Review documents	Video	Labs	My experience
Cloud IAM	Cloud IAM which lets you manage access control by defining *who* (identity) has *what access* (role) for *which* resource.	1- Best way to manage (use groups) 2- Roles (primitive, predefined & custom) 3- Roles necessary to do certain functions 4- Password min requirements	How IAM works Create a strong password Modern password security Roles Service account constraints Limit spoofing threats	What is Cloud IAM Better Practices for Cloud IAM	Cloud IAM: Qwik Start Custom Roles Service Account Roles	Core component of security integrated across all services. Check out the concept of constrains and service accounts.
2FA	Two factor authentication is an added layer of security to secure your identities.	1- Recovery with 2FA 2- MFA Multiple factor authentication. 3- Account you should use MFA on 4- OS login 2FA	Protect your business with 2FA OS Login with 2FA Recovery acc protected by 2fa	How to choose the right 2FA		Understand the various uses of 2FA and which account should always be secured.
Identity Aware Proxy	Cloud Identity-Aware Proxy (Cloud IAP) controls access to your cloud applications and VMs running on (GCP)	1- How it works (HTTPS) 2- JWT (signed headers) 3- How to configure 4- On prem flow 5- TCP forwarding 6-IAM roles	- Identity-Aware Proxy overview - Securing your app with signed headers -IAP for on-premises apps	Centralize access to your organization's websites with Identity Aware Proxy (IAP) Beyond Corp	User authentication with Identity-Aware Proxy	Understanding the flow is important and where and when to use it. That makes the difference in selecting the correct answer if it isn't obvious. TCP forwarding understand concept.
Google security model	Google's end to end security process built up over 15+ year to secure their various offering including Google Cloud Platform	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	Trust and Security Google security whitepaper PCI DSS shared security model	Security and compliance Shared Responsibility: What This Means for You as a CISO		Nice section to get asked about. Check the compliance standard like PCI, HIPPA, ISO 27001, 27017, 27018

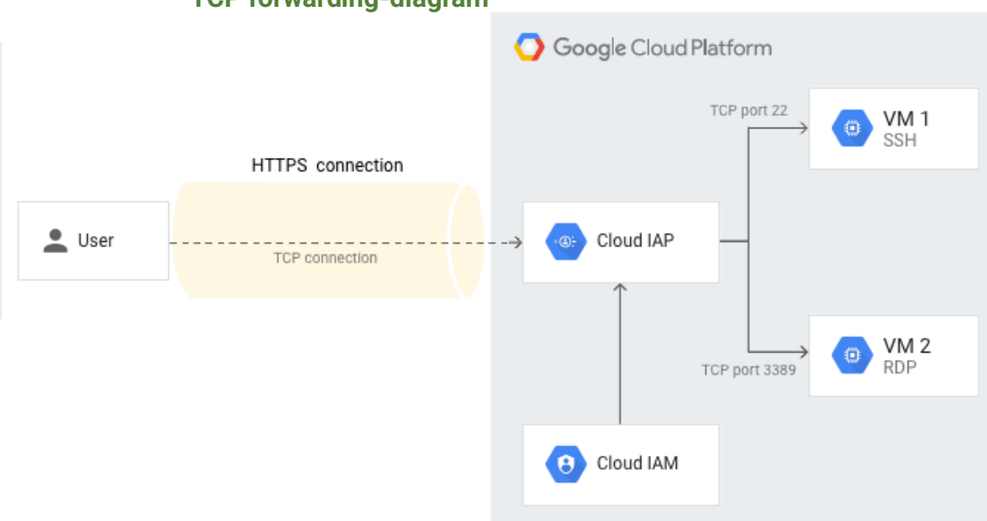
Cloud IAP flows - diagram



On Prem flow - diagram

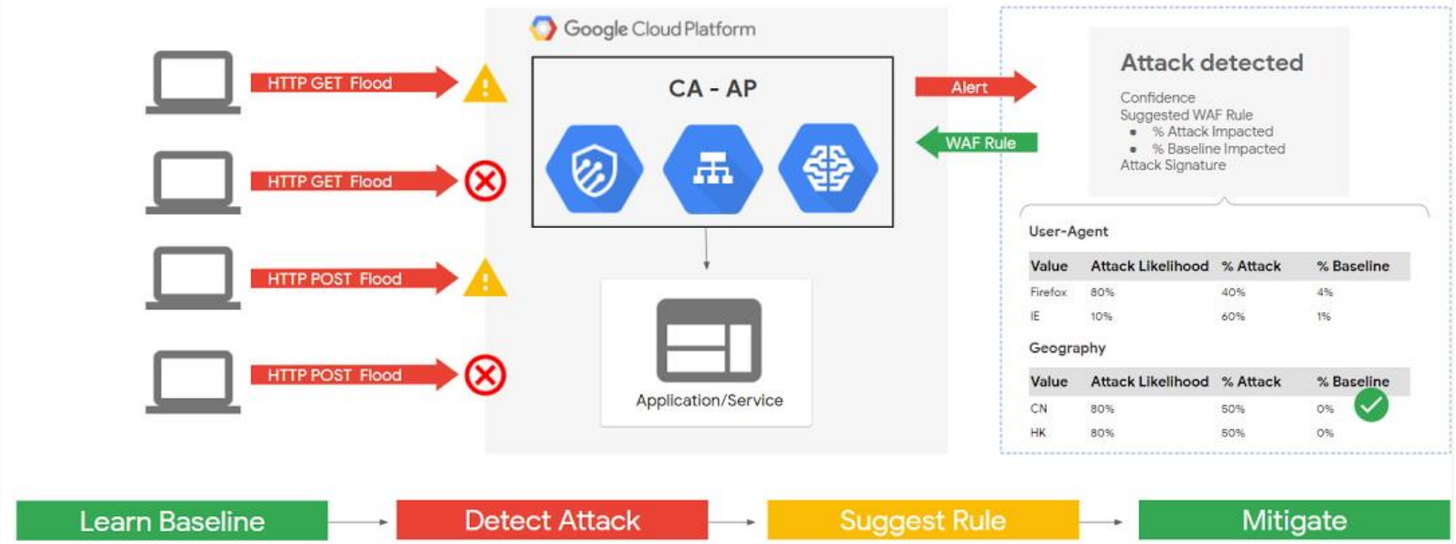


TCP forwarding-diagram



VPC	**What it is** A VPC network, is your virtual network in the cloud just like an on prem physical network or data centre or office network.	**What you should know** 1- 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**	**Video** **VPC's** **Securing Data with VPC service control**	**Labs** **Multiple VPC networks**	**My experience** Can't have security without networking understand very well. Understand service control also.
Default VPC	**What it is** Default network is created by default when you create a project.	**What you should know** 1- Default network 2-How do disable it	**Review documents** **VPC default network**			**My experience** Securing your VPC can be done in various ways. One such way is using constraints. Take a look at a few common ones.
Migrating projects	**What it is** Migrating project can occur and is not out of the way.	**What you should know** 1- How to migrate projects 2- How to handle permission and constraints on projects that are to be migrated	**Review documents** **Migrating projects**			**My experience** Migration can get tricky especially if there are various security elements applied on the project. Check out the flow.
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, Default rules 3- Firewall hierarchy 4- Effect of sharing, peering, etc 5- Filtering methods (IP, Tags, SA)	**Review documents** **Implied rules** **Filtering by service accounts** **Firewall hierarchy**	**Video** **How firewall protect your environment** **Firewall Insights**	**Labs** **VPC Networks - Controlling Access**	**My experience** There are some implied and default rule know these. Also, how to define your rules (source, dest, port, 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) 3- Restrictions Cloud armour and CDN 4- Security policy requirements	**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. Know this may get you a point or 2.
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.
NGFW	**What it is** A centralized set of firewalls run as virtual machines that deliver features	**What you should know** 1- How to configure 2- Filter traffic 3- reasons to use	**Must review documents** **Centralized network appliances on Google Cloud** **Deploying FortiGate-VM Next Generation Firewall**			**My experience** Get familiar

Cloud Armor - diagram



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. (25, 43, 110, 143,195, 443, 465, 587, 700, 993, 995, 1883, and 5222)	**What it is** Load balancer for TCP without SSL. (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. (any port)	**What it is** Load balancer for TCP /UDP regional, Internal traffic (any port)

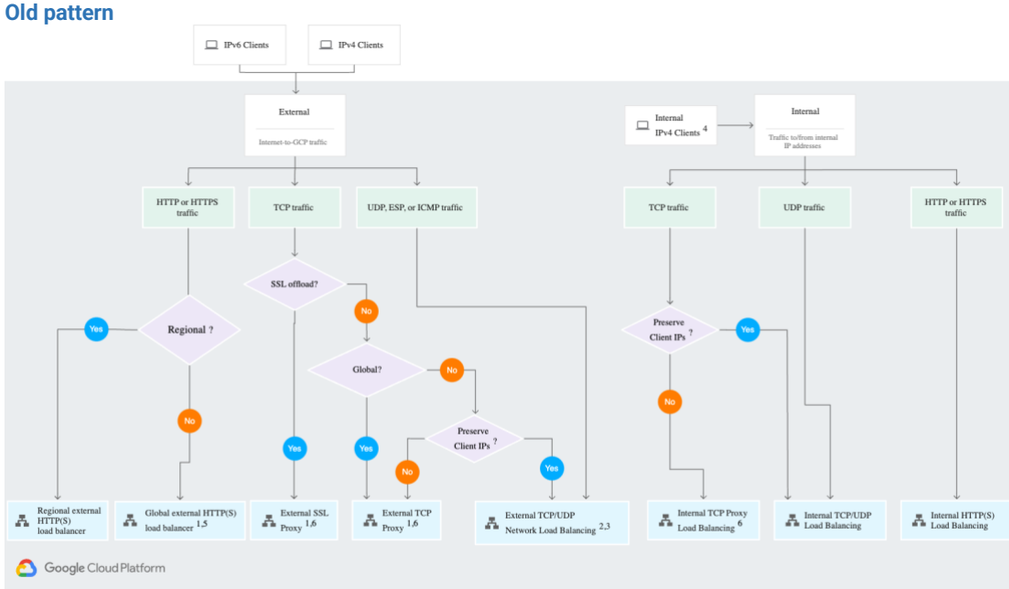
Review documents
Choosing a load balancer

Note: Load balancer types updated in 2023 now (Application and Network)

Video
Cloud Load balancers

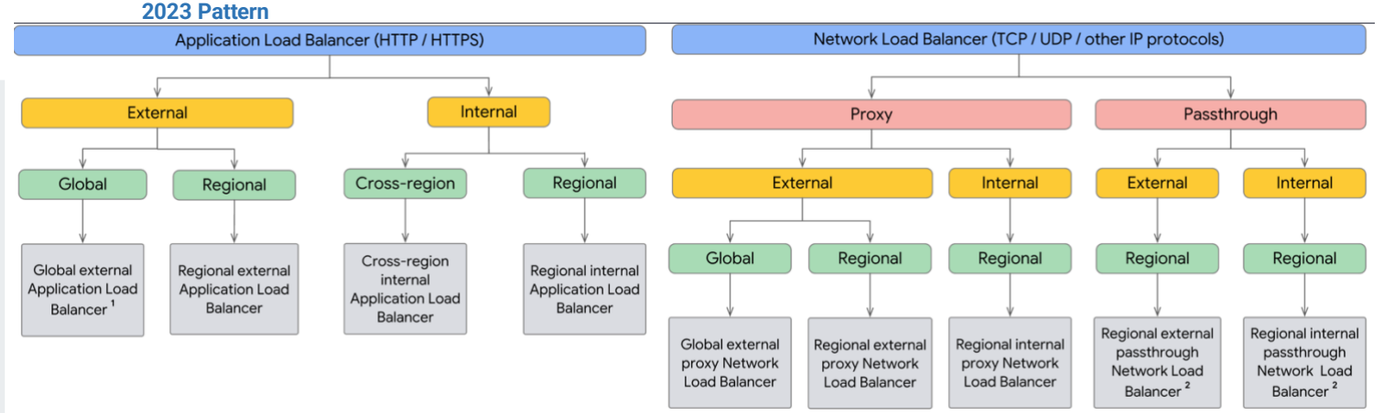
My experience
This is tricky so know the main points (Global vs Regional, External vs Internal, Traffic type)

Old pattern

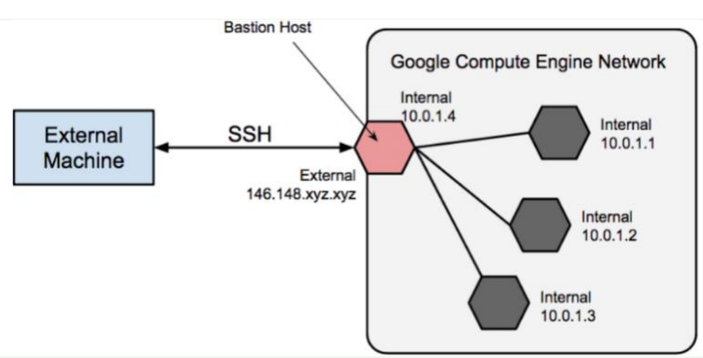


[1] IPv6 termination is available if you configure the load balancer in Premium Tier.
[2] Choose external TCP/UDP network load balancing if you need to ensure that the load balancer is located in a particular region, or if you want to configure IPv6 load balancing (with dual-stack backends). The latter is only available for backend service-based network load balancers.
[3] External TCP/UDP network load balancers use regional external IP addresses that are accessible by clients anywhere.
[4] Clients in a VPC network or in a network connected to a VPC network.
[5] The global external HTTP(S) load balancer (classic) can be configured to be effectively regional in Standard Tier.
[6] Client source IP preservation is available in certain configurations by using the PROXY protocol.

2023 Pattern

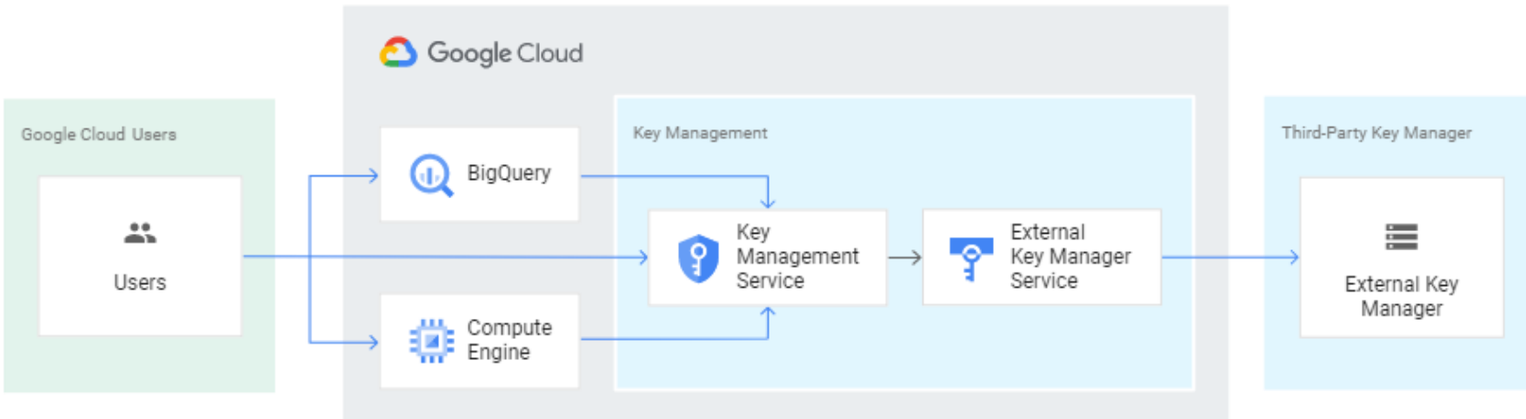


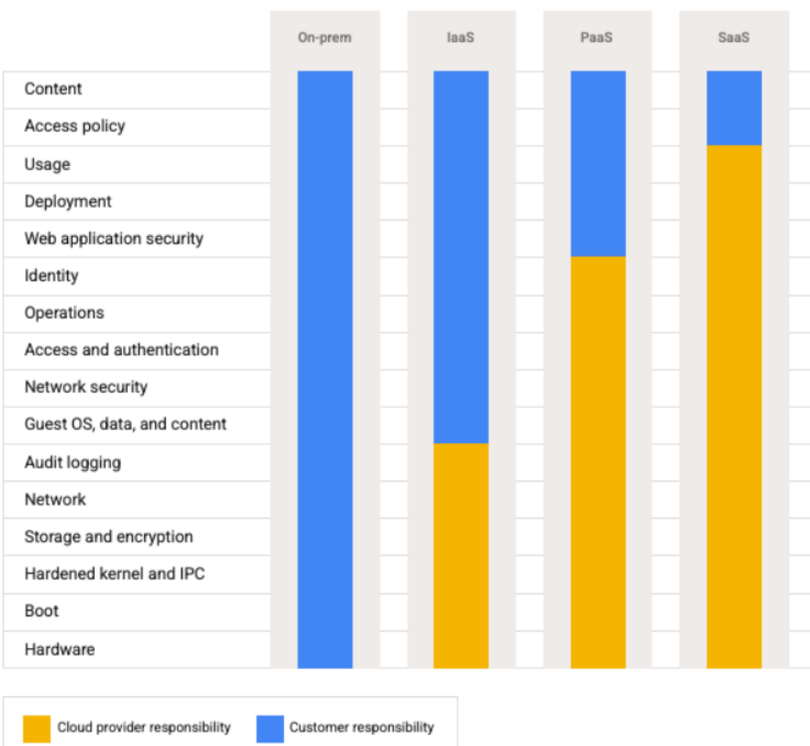
VPC Sharing	VPC Peering	VPN	Dedicated Interconnect	Partner Connect	Review documents
					▪ **Hybrid connectivity options** ▪ **Shared VPC overview**
What it is Used to connect to a common VPC network. Resources in those projects can communicate with each other securely and efficiently across project boundaries using internal IPs.	**What 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 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 it is** Use dedicated Interconnect to connect to Google's network through a highly available, low latency connection. (10GB higher)	**What it is** Use Google Cloud Interconnect - Partner (Partner Interconnect) to connect to Google through a supported service provider. (from 50 MB up)	**Video** **Connectivity Hybrid** **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?
What you should know 1- Centralised management 2- Firewall control 3 – internal RFC1918	**What you should know** 1- When to peer what 2 - services you have access to	**What you should know** 1- Over internet 2 – IPSEC used 3 – dynamic setup	**What you should know** 1- Reason to use this 2- Min 10GB 3 – Not over the internet	**What you should know** 1- Best case use 2 – Min size 50MB 3 – Not over the internet	
DNS SEC	Private Access	Cloud NAT	Bastion Host	Mirror ports	Review documents
					▪ **DNSSEC** ▪ **Cloud NAT** ▪ **Private Access** ▪ **Private access on prem**
What it is Prevents attackers from manipulating or poisoning the responses to DNS requests.	**What it is** Allows VM instances with internal (**RFC 1918**) IP addresses to reach certain APIs and services without internet access.	**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 it is** Bastion hosts provide an external facing point of entry into a network containing private network instances from the Internet	**What it is** Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination.	**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.
What you should know 1- What it protects	**What you should know** 1- How to enable 2- Restricted and private 3- Configure for on prem envs and cloud 4- **DNS config**	**What you should know** 1. How it works	**What you should know** 1- Where it sits	**What you should know** 1- **How it works**	



Cloud KMS	CMEK	CSEK	Cloud EKM	Cloud HSM	Review documents
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 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 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 it is** With Cloud EKM, you can use keys that you manage within a supported external key management partner to protect data within Google Cloud. You can protect data at rest in supported CMEK integration services, or by calling the Cloud Key Management Service API directly.	**What it is** You can generate encryption keys and perform cryptographic operations in FIPS 140-2 Level 3 certified HSMs	▪ **Customer managed encryption keys (CMEK)** ▪ **Customer supplied encryption keys (CSEK)** ▪ **Envelop encryption** ▪ **EKM** ▪ **Cloud HSM**
What you should know 1- It's purpose 2- What are the cases you should use it.	**What you should know** 1- What products support this service (BigQuery, Cloud Build, Cloud Dataproc, Cloud Storage, Compute Engine) 2 – Know the step 3- gcp.restrictNonCmekServices	**What you should know** 1- Supported by Compute and Cloud storage 2 – This key replaces the KEK 3 – Know the step (very important)	**What you should know** 1- How to configure the steps 2 - What cases to use it 3 - Know the step (very important) 4 - Key access Justification	**What you should know** 1- Where to use it 2 - Meets FIPS Level 3 requirement 3 - How it works	**Video** - **KEYS** **EKMS and KAJ** **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. You will get questions on this. Know all situations, and which key type is used & most importantly, which products support which type. Know like the alphabet.
Key rotation	Managing secrets	DLP	DLP cryptographic methods	Crypto-delete	Review documents
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 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 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 these are** These are AES-SIV, FPE-FFX, HMAC.	**What it is** Crypto-deletion, or crypto-shredding, is the process of rendering data unrecoverable by deleting the key used to encrypt it. Since the data can no longer be decrypted, it is effectively deleted	▪ **REGEX** ▪ **Pseudonymization** ▪ **DLP** ▪ **Cryptographic methods** ▪ **Transformation** ▪ **Secret manager** ▪ **Key rotation** ▪ **Crypto-delete aka crypto-shredding** **Video:** **DLP** **Secret manager** **My experience**
What you should know 1- Reason to rotate keys 2- Method automatic or manual, regular, irregular 3 – Commands	**What you should know** 1- Choosing a secret management solution 2 – Rotating secrets	**What you should know** 1-How it works (Redact, Crypto-based, Masking, date shifting) 2 - How to configure and regex 3- Reversible vs Non reversible DLP (know which methods do what) 4- CloudStorageRegexFileSet	**What you should know** Spend some time to understand what methods help you achieve what. What's reversible and what's not.	**What you should know** 1- Know what it does and how it works	DLP should be well known especially how to achieve various results. This topic is tricky spend some time on it.

Cloud EKM diagram

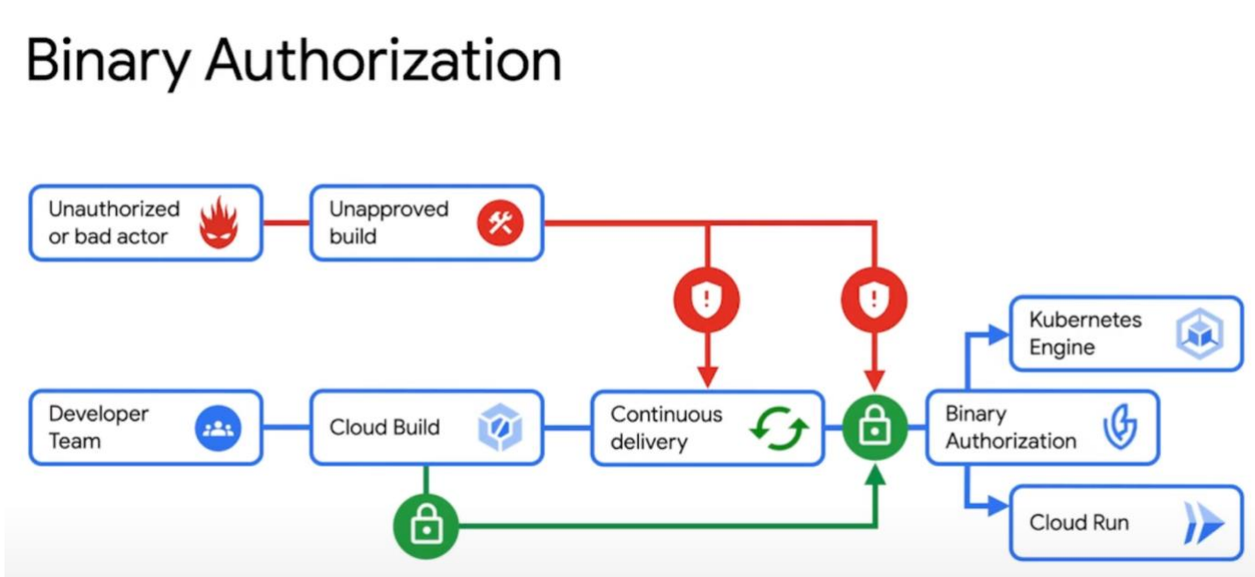




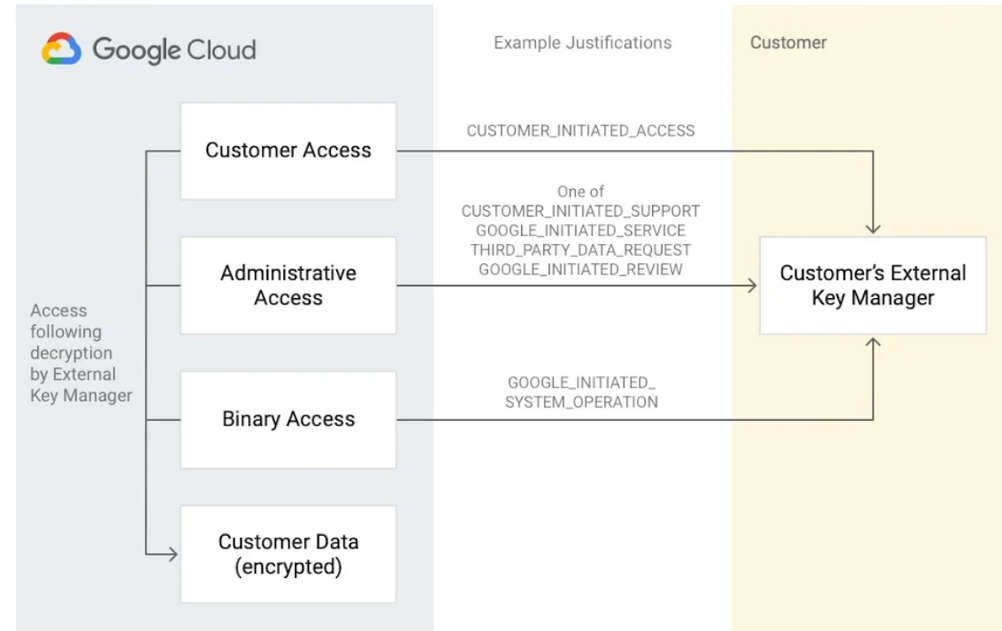
Data Sovereignty	Kubernetes	G Suite	Web Security Scanner	Security Command Center	Review documents
What it is Data residency and sovereignty requirements are based on your regional and industry-specific regulations, and different organizations might have different data sovereignty requirements	**What it is** The Kubernetes networking model relies heavily on IP addresses. Services, Pods, Containers, and nodes communicate using IP addresses and ports.	**What it is** Google's SaaS offering comprised of Gmail, Docs, Drive, Calendar, Meet and more for business.	**What it is** The Cloud (Web)Security Scanner identifies security vulnerabilities in your App Engine, Compute Engine and Google Kubernetes Engine web applications.	**What it is** Security Command Center lets you filter and view vulnerabilities and threat findings in many different ways, like filtering on a specific finding type, resource type, or for a specific asset.	▪ **Web Security Scanner** ▪ **Security Command Center** ▪ **Data Sovereignty** ▪ **7 best practices for building containers** ▪ **Kubernetes** ▪ **Container threat detection** ▪ **Event Threat Detection** ▪ **Container analysis** ▪ **RBAC GKE** **Video** ▪ **GKE security basics** ▪ **Security Command Center Playlist** ▪ **KUBERNETES** ▪ **GKE shared security**
What you should know 1- Enforce residency and operational sovereignty Video **Meeting your digital sovereignty**	**What you should know** 1- How it works 2- Containers and pods 3- How to secure 4- Updating 5- **GKE security Basics**	**What you should know** 1-High level administration 2 - Managing users, setting up domain, IAM, Super user account	**What you should know** 1- Reason to use this **Lab** **Web Security Scanner: Qwik Start**	**What you should know** 1- The components Web security scanner, VM manager, Container Threat Detection, Event Threat Detection 2-Crypto mining protection with Virtual Machine Threat Detection 3- Mute findings 4- Security Health Analytics vulnerability 5 - Patch management	**Labs** **Mitigate Threat with SCC** **My experience** Important for the exam

Binary authorization	**Key Access Justification**	**Cloud IDS**	Policy Intelligence		Review documents
What it is Binary Authorization is a deploy-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE) or Cloud Run	**What it is** Key Access Justifications provides a reason every time your externally managed keys are accessed	**What it is** Provides cloud-native network threat detection with industry-leading security.	**What it is** Helps enterprises understand and manage their policies to reduce their risk. By providing more visibility and automation, customers can increase security without increasing their workload		▪ **Binary authorization** ▪ **Key Access Justification** ▪ **Policy Analyzer** **Video** **Policy Intelligence** **Cloud IDS**
What you should know 1- How it works 2 - How to enforce 3 - With VPC service controls Lab GKE: Binary Authorization	**What you should know** 1- Use cases for this	**What you should know** 1- General awareness **Lab** **Cloud IDS**	**What you should know** 1- How it works 2 – Components, Policy Troubleshooter, Policy Analyzer, Policy Simulator		

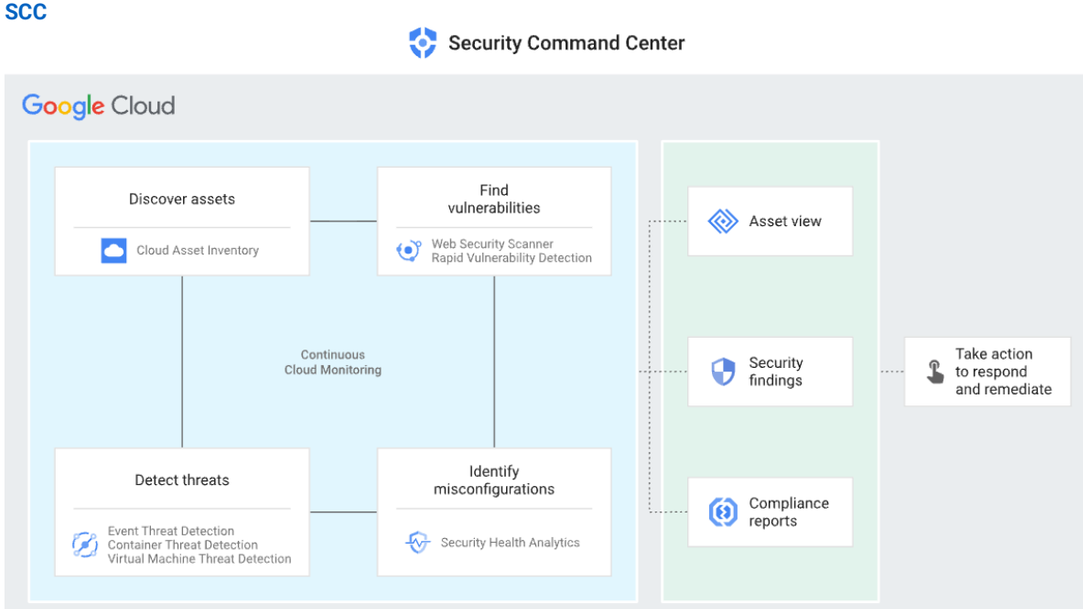
Binary authorization



KAJ and EKM



SCC



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
What you should know 1- Authorised views 2- How to export data 3-- Cloud DLP 4- **Keys CMEK**	**What you should know** 1-Types (nearline, coldline) Object storage. 2- Encryption options (default, CSEK, CMEK) 3- How to retain Data 4- Migrate Data 5- Public access prevention	**What you should know** 1- Secured images 2- How to secure access 3- How to update 4- **Secure image pipeline** 5- **Shielded VM** 6- **Confidential VM**	**What you should know** 1- Used for compliance 2- Used for security analytics 3- Used for SIEM 4- Log sink for Org 5- set default location for logging	**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
What you should know 1- What they are used for 2- Recommended limits 3- 2FA 4-Discourage use	**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 Events 3- Admin Activity 4- Transparency Access Logs

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**
- **BigQuery Column—level security**
- **Row level security**
- **Encryption BigQuery**

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.

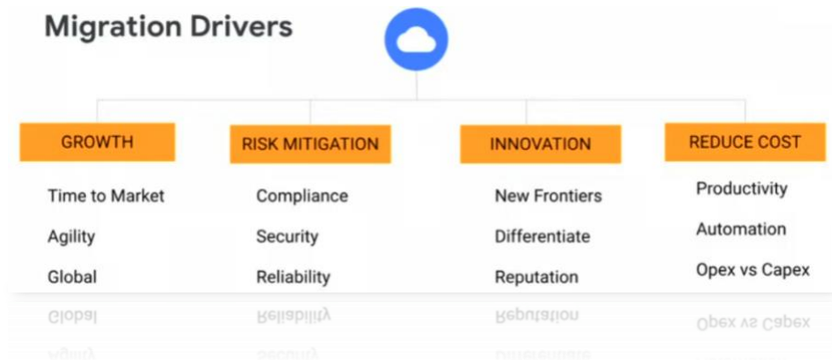
Review documents

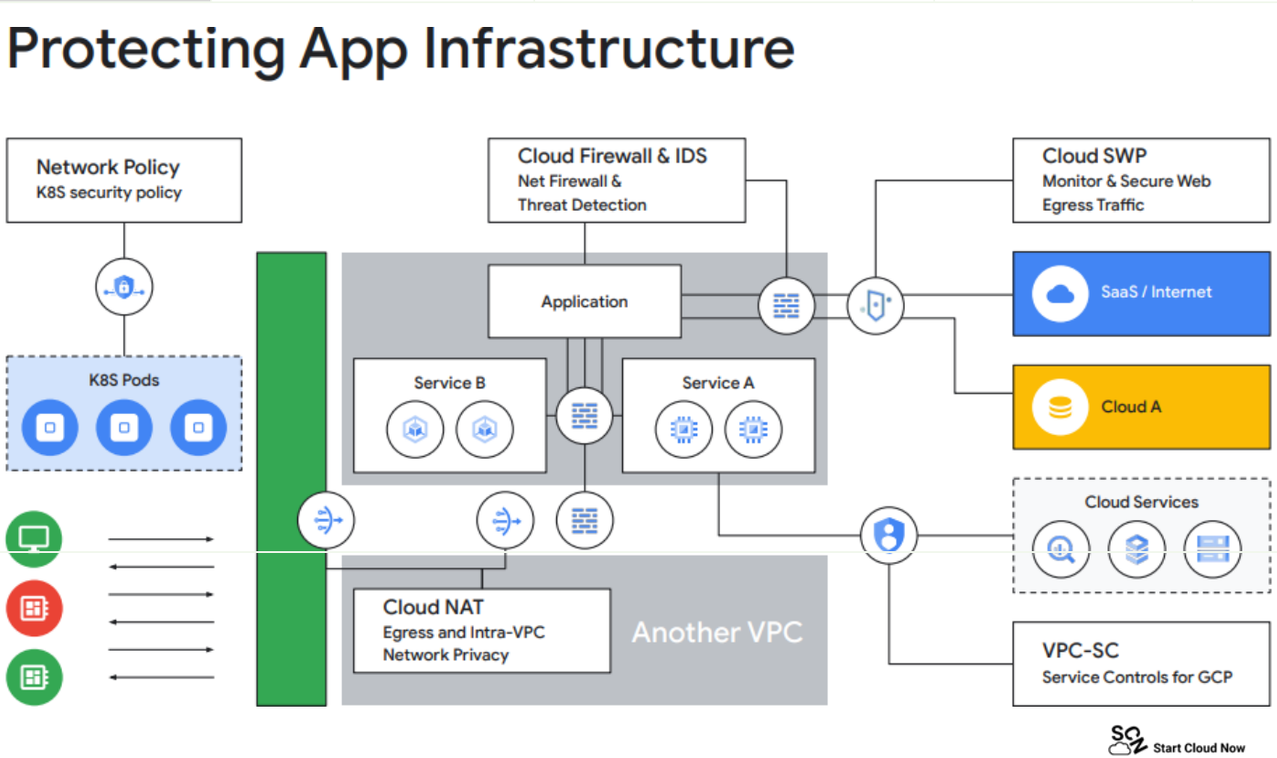
- **DNS Security Extensions (DNSSEC)**
- **DDoS**
- **AppEngine**
- **Access Transparency Log**
- **Type of audit logs**

Video
DDoS
AUDIT LOGS

My experience
Be familiar with types of access certain accounts have, deployment methods, types of audit logs you may need. Restricting access by Google personnel my pop up.

private.googleapis.com	**What it is** Use **private.googleapis.com** to access Google APIs and services using a set of IP addresses only routable from within Google Cloud.	**What you should know** 1- Choose when you don't use VPC Service Controls. 2- Choose when you do use VPC Service Controls, but you also need to access Google APIs and services that are not supported by VPC Service Controls. 3- **199.36.153.8/30**	Review documents **configure**	**My experience** Some tricky stuff here.
restricted.googleapis.com	**What it is** Use **restricted.googleapis.com** to access Google APIs and services using a set of IP addresses only routable from within Google Cloud.	**What you should know** 1- Choose when you only need access to Google APIs and services that are supported by VPC Service Controls 3- **199.36.153.4/30**		
Firewall Insights	**What it is** Firewall Insights helps you better understand and safely optimize your firewall rules	**What you should know** 1- Part Network Intelligence Center 2- What's it's used for	Review documents **Firewall Insights**	





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

By *Ammett:*