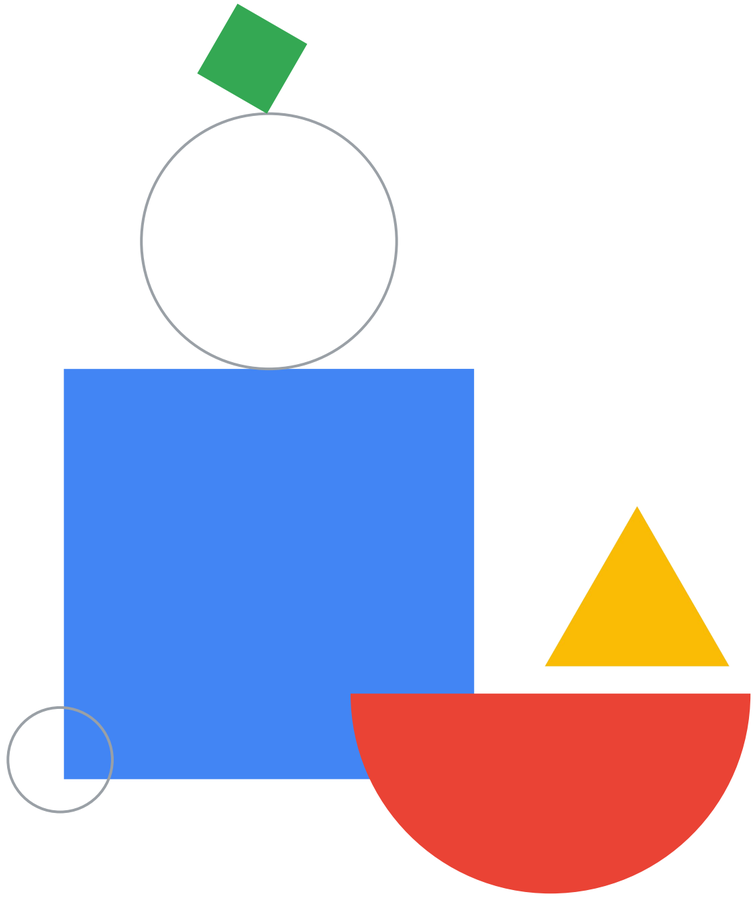
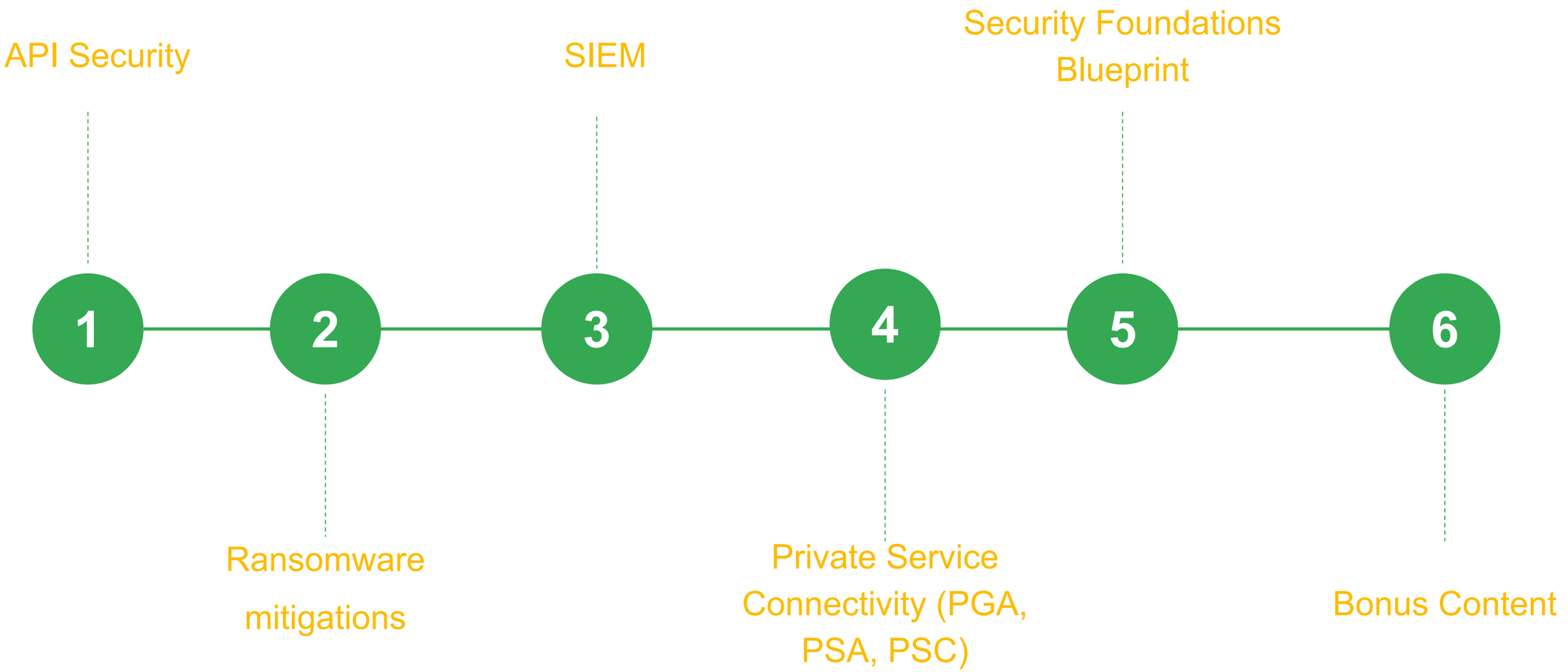
Google Cloud

Preparing for Your Professional Cloud Security Engineer Journey



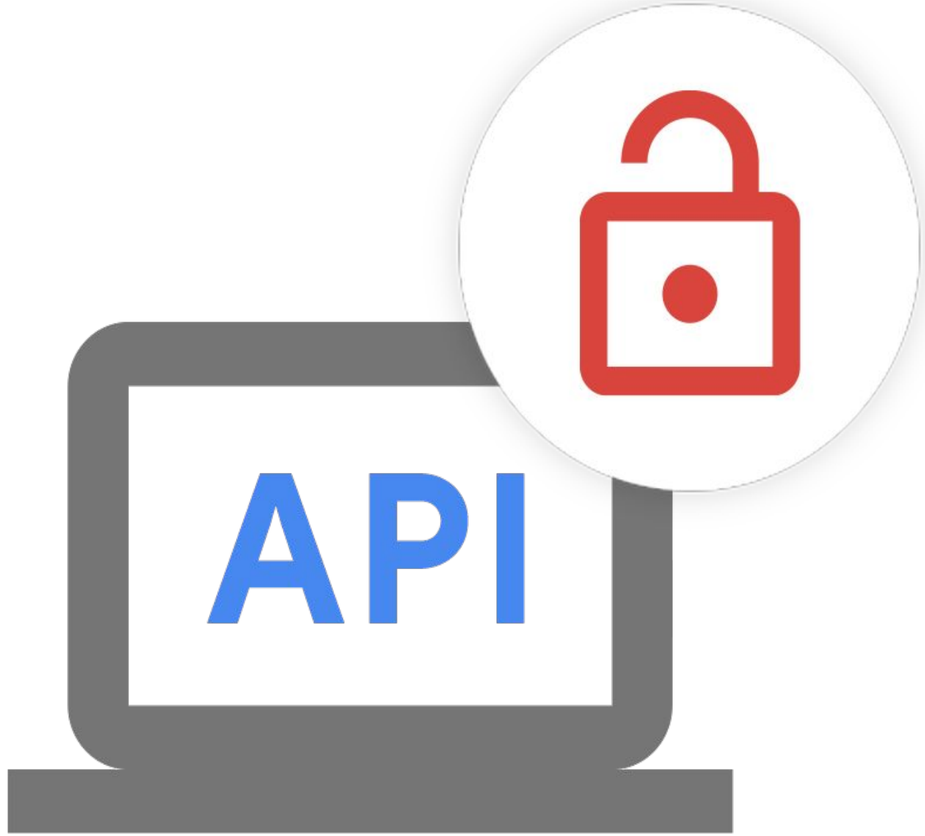
Week 6 topics



API Security

Security perspective: APIs are under attack

- Denial of Service attacks
- Brute force attacks
- Bots probing for API security weakness
- Competitors scraping price data
- Credential stuffing
- Abuse of guest accounts
- Bot traffic skewing analytics and KPIs
- Authentication and authorization attacks
- Dictionary-type attacks
- Man-in-the-Middle attacks
- SQL Injection Attacks



API security: solution using Google managed products

Apigee
API management

OAuth 2 & SAML

API Keys

RBAC management

Cloud Armor
Web Application Firewall

DDoS protection

Geo-fencing of APIs

Mitigate OWASP Top 10 risks

Ransomware mitigations

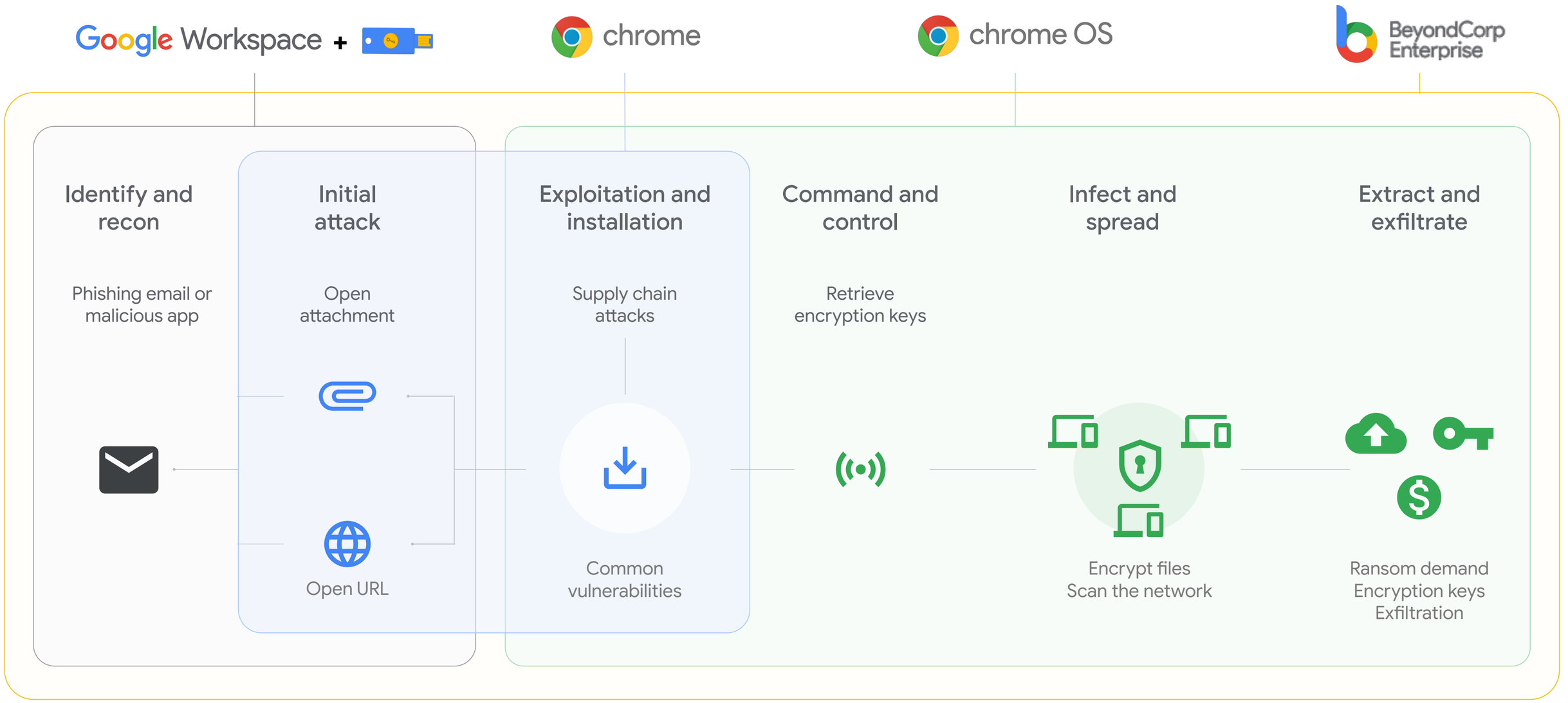
End-user protection

Gmail automatically prevents many malicious attacks from reaching inboxes.

Google Safe Browsing identifies dangerous links.

Google Drive scans files for malware.

The Google security stack at work against ransomware



GCP Ransomware mitigations

- Google Cloud provides multiple layers of protection.
- Most protections are automated and available by default.
- This is what you can do on top of it.

Unique Crypto Mining Protection backed with a $1M Credit Warranty

Cryptojacking is a prevalent cyber attack for all cloud vendors.

If Google Cloud fails to detect a cryptomining attack, we will issue up to $1M of credits to cover the compute expenses resulting from the attack*

Google Cloud

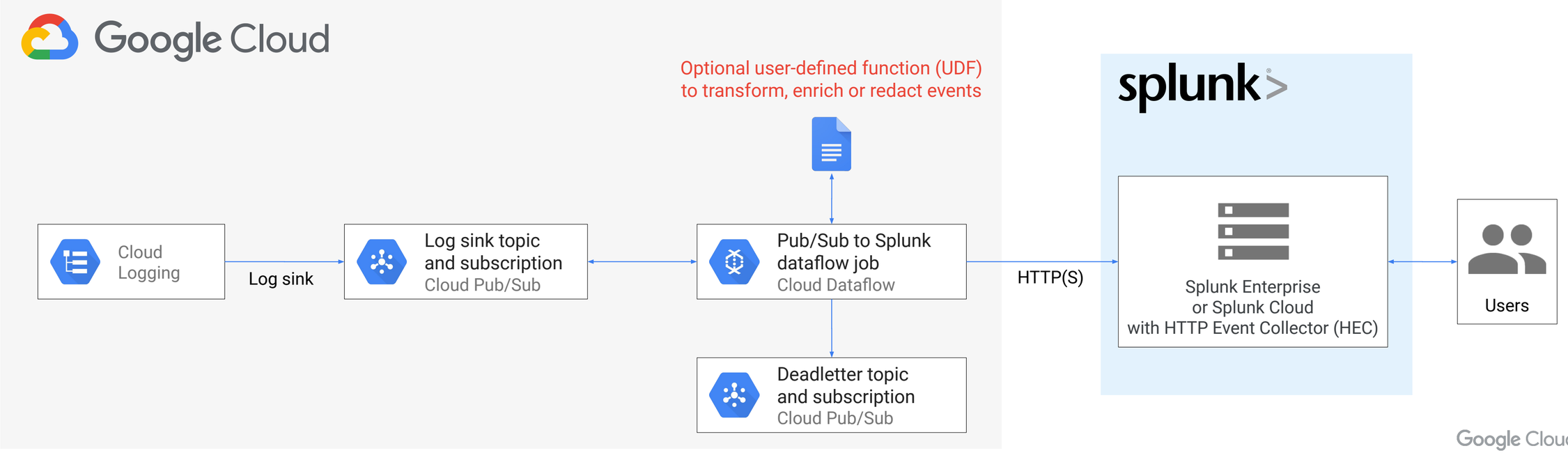
65%

When a user loses access to their account on GCP 65% of the time the attacker uses the stolen access for CryptoJacking

SIEM

3rd party SIEM (and SOAR): GCP integrations

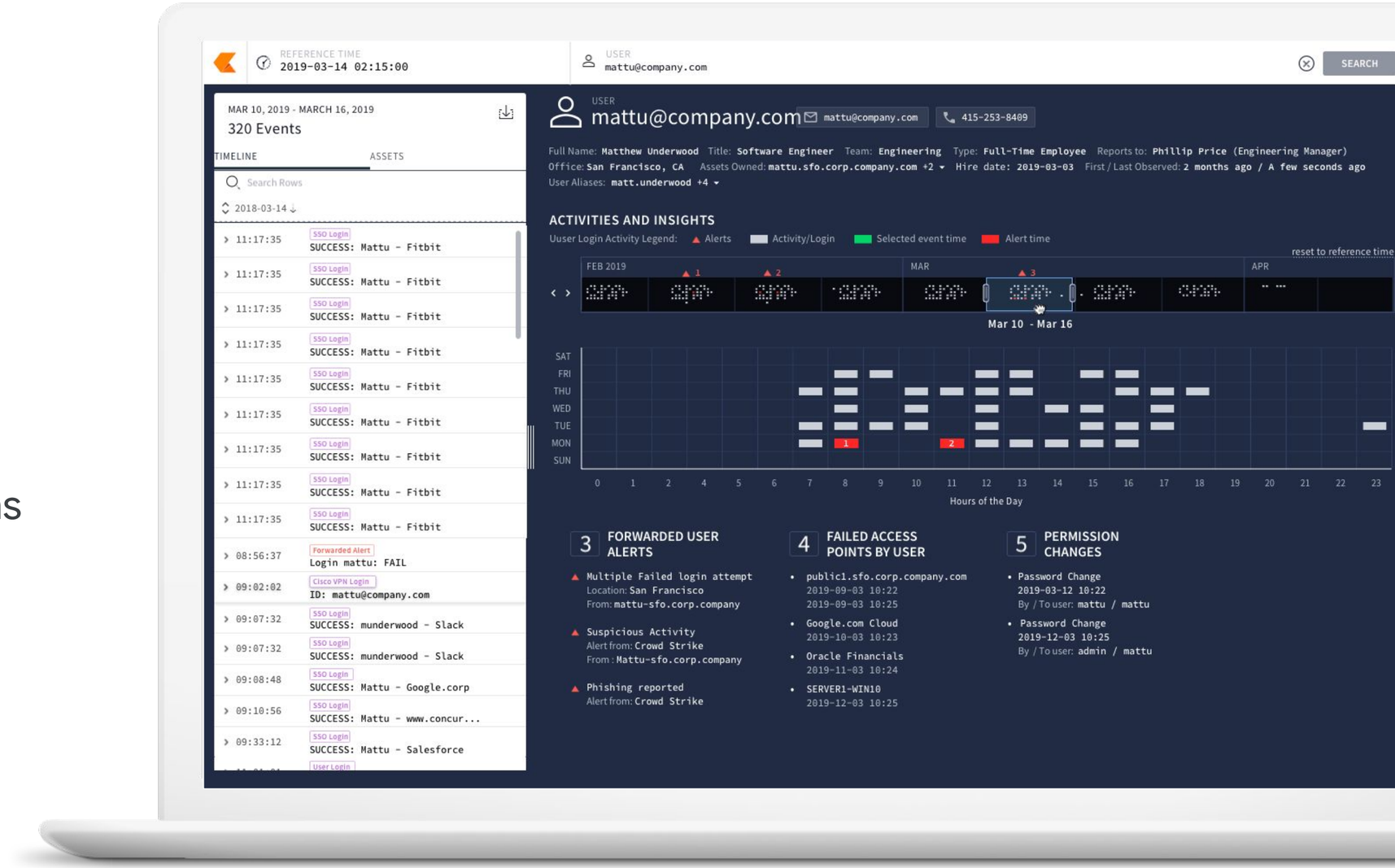
- Splunk
- Datadog
- Exabeam
- Qradar
- Sentinel
- And more…



Chronicle

A **cloud-native** security information and event management (SIEM) solution.

Designed to enable security teams to **detect, investigate and respond to threats** at Google speed and scale.



2022-08-16T22:04:00.000Z

Enter a hostname, domain, IP, URL, email, username, or file hash

SEARCH

LOGGED IN AS
sharat.ganesh@1823127835827.…

RULES DASHBOARD | RULES EDITOR | CHRONICLE RULES NEW

12/14 ENABLED RULE SETS

As of today

- Rule sets with precise rules enabled 12/12
- Rule sets with broad rules enabled 12/12

MOST ACTIVE RULES

Over last 7 days

- Empire Powershell stager launch +10019
- Powershell Obfuscation Technique: Bitwise XOR +4
- Powershell execution with encoded commands or execution policy variants +4
- Base64 Encoded Base64 in Powershell +4

MOST ACTIVE RULE SETS

Over last 7 days

- RAT +10019
- Suspicious Behavior +12

RULE SETS | DASHBOARD | QUICK ACTIONS

Chronicle rules offer preconfigured detection logic to uncover threats. Learn more about Chronicle rules.

Last refreshed: a few seconds ago

NAME ↑	LAST UPDATED	ENABLED RULES	ALERTING	MITRE TACTICS	MITRE TECHNIQUES
Cloud Threats • 3 Rule sets					
Admin Action	2022-07-26	P B	P B	T1078 TA0003	T1037.005 T1078.004 +2 more
Potential Exfil Activity	2022-07-13	P B	P B	TA0011	T1071.004
Weakened Config	2022-08-11	P B	P B	None	None
Managed Detection Testing • 2 Rule sets					
GCP Managed Detection Testing	2022-07-15	Disabled	Off	None	None
Windows Managed Detection Testing	2022-07-14	Disabled	Off	None	None
Windows Threats • 9 Rule sets					
Crypto Activity	2022-07-01	P B	P B	TA0002 TA0003	T1053 T1562
Hacktool	2022-07-01	P B	P B	TA0002 TA0004 +1 more	T1047 T1059 +3 more
Info Stealer	2022-07-22	P B	P B	TA0007 TA0009	T1482 T1560
Initial Access	2022-07-29	P B	P B	TA0002 TA0003 +3 more	T1055 T1059 +11 more

What We Solve: Security Data Overload

SIEM Challenges

Can't scale
Legacy platforms were not built for petabyte scale

Too expensive
Ingestion based pricing forces customers to limit what is collected and retained

Misses threats
Incomplete data, Teams unable to see relationships between malicious indicators and events across time

Chronicle Security Analytics

Cloud-native:
Operate at Google scale and speed

Fixed Cost:
No penalty for analyzing everything

Clear Signals:
Curated intel X enriched telemetry X YARAL

4.2 Diagnostic Question 08 Discussion

Cymbal Bank has suffered a remote botnet attack on Compute Engine instances in an isolated project. The affected project now requires investigation by an external agency. An external agency requests that you provide all admin and system events to analyze in their local forensics tool. You want to use the most cost-effective solution to enable the external analysis.

What should you do?

A. Use Event Threat Detection. Trigger the IAM Anomalous Grant detector to detect all admins and users with admin or system permissions. Export these logs to the Security Command Center. Give the external agency access to the Security Command Center.

B. Use Cloud Audit Logs. Filter Admin Activity audit logs for only the affected project. Use a Pub/Sub topic to stream the logs from Cloud Audit Logs to the external agency's forensics tool.

C. Use the Security Command Center. Select Cloud Logging as the source, and filter by category: Admin Activity and category: System Activity. View the Source property of the Finding Details section. Use Pub/Sub topics to export the findings to the external agency's forensics tool.

D. Use Cloud Monitoring and Cloud Logging. Filter Cloud Monitoring to view only system and admin logs. Expand the system and admin logs in Cloud Logging. Use Pub/Sub to export the findings from Cloud Logging to the external agency's forensics tool or storage.

4.2 Diagnostic Question 08 Discussion

Cymbal Bank has suffered a remote botnet attack on Compute Engine instances in an isolated project. The affected project now requires investigation by an external agency. An external agency requests that you provide all admin and system events to analyze in their local forensics tool. You want to use the most cost-effective solution to enable the external analysis.

What should you do?

A. Use Event Threat Detection. Trigger the IAM Anomalous Grant detector to detect all admins and users with admin or system permissions. Export these logs to the Security Command Center. Give the external agency access to the Security Command Center.

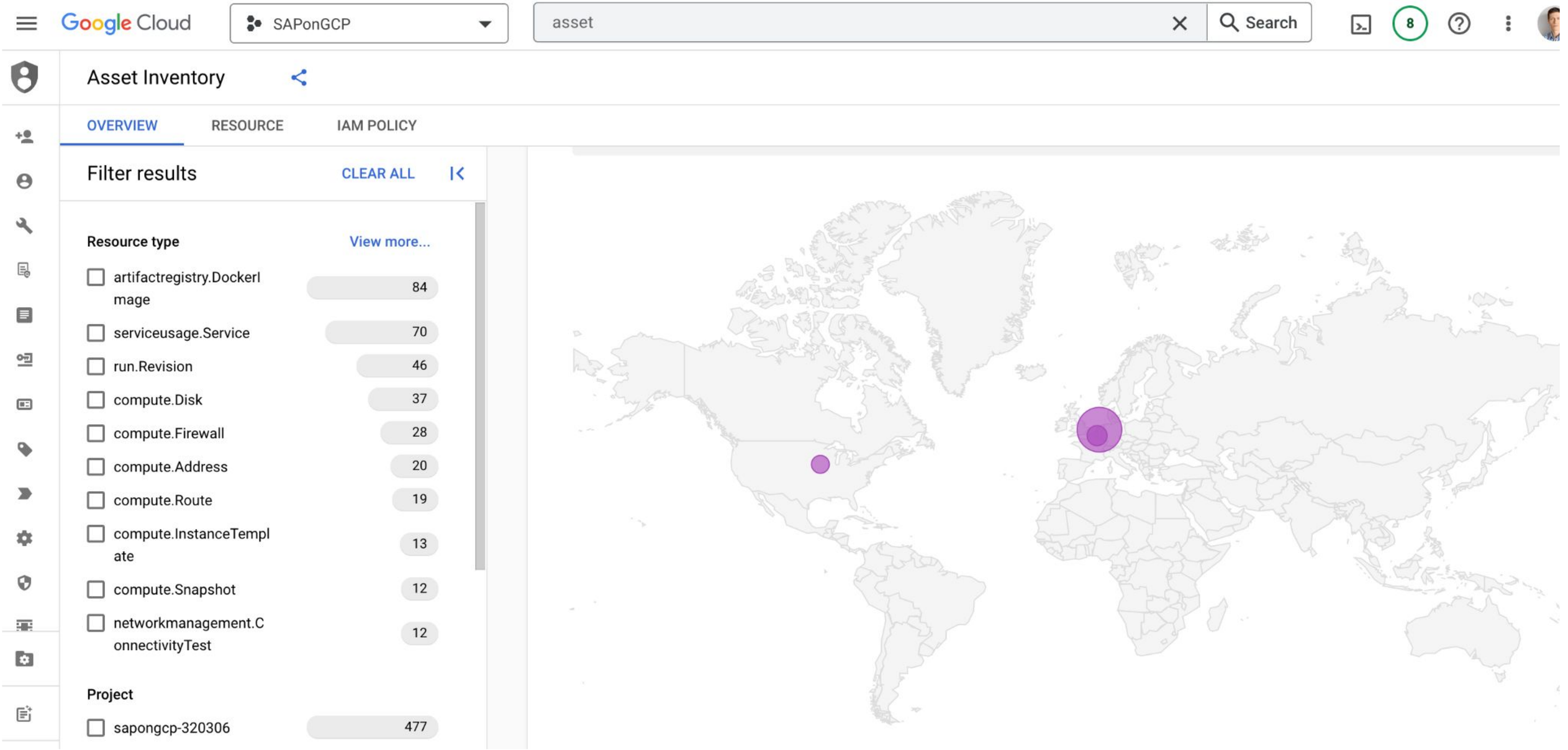
B. Use Cloud Audit Logs. Filter Admin Activity audit logs for only the affected project. Use a Pub/Sub topic to stream the logs from Cloud Audit Logs to the external agency's forensics tool.

C. Use the Security Command Center. Select Cloud Logging as the source, and filter by category: Admin Activity and category: System Activity. View the Source property of the Finding Details section. Use Pub/Sub topics to export the findings to the external agency's forensics tool.

D. Use Cloud Monitoring and Cloud Logging. Filter Cloud Monitoring to view only system and admin logs. Expand the system and admin logs in Cloud Logging. Use Pub/Sub to export the findings from Cloud Logging to the external agency's forensics tool or storage.

Asset Inventory

Cloud Asset Inventory replaces Forseti



Private Connectivity Options

Managed services connectivity methods

Private Google Access (PGA)	Private Services Access (PSA) with VPC Peering	Private Service Connect (PSC) for Google APIs and Google Managed Services (future direction)	VPC Serverless Connectors
Access Google APIs (ex: Cloud Storage or BigQuery) privately, from Google Cloud or on-prem	Privately connect producer and consumer VPCs via VPC peering (e.g.: Google managed VPC for Cloud SQL)	Privately connect producer and consumer VPCs with Private Service Connect (scales to hundreds or thousands of services shared)	Provides connectivity to Google Cloud Serverless services (App Engine Standard, Cloud Function, Managed Cloud Run) to resources in your VPC

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

You need to know when to use which one!

Private Google access

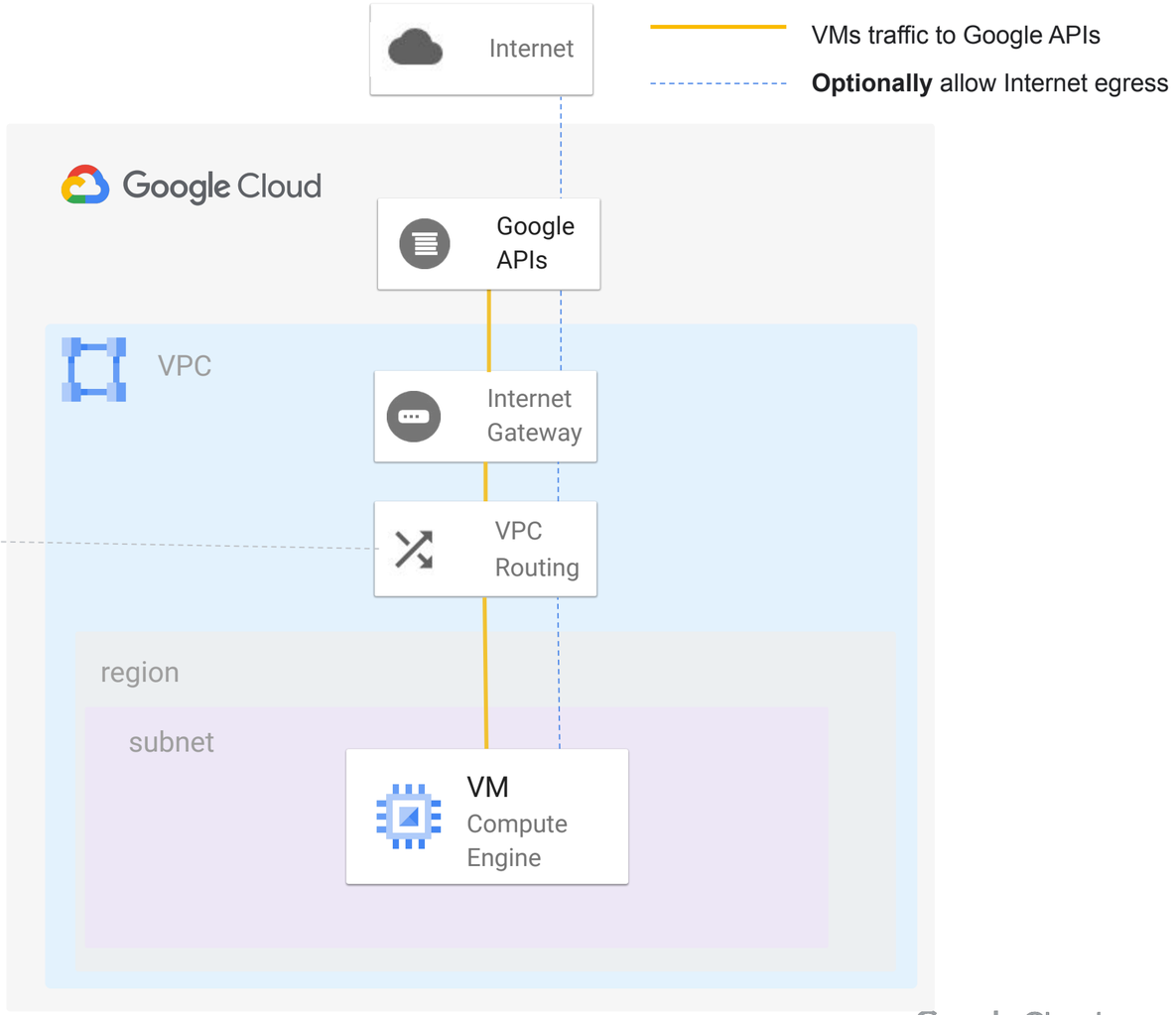
Allow Google Cloud VMs to reach API endpoints, without Internet access.

Problem:

Instances without access to the Internet can't access Google Cloud public API endpoints.

Solution:

Enable **Private Google Access** in the subnetwork the instance is attached to.



Example of Google API based managed services:

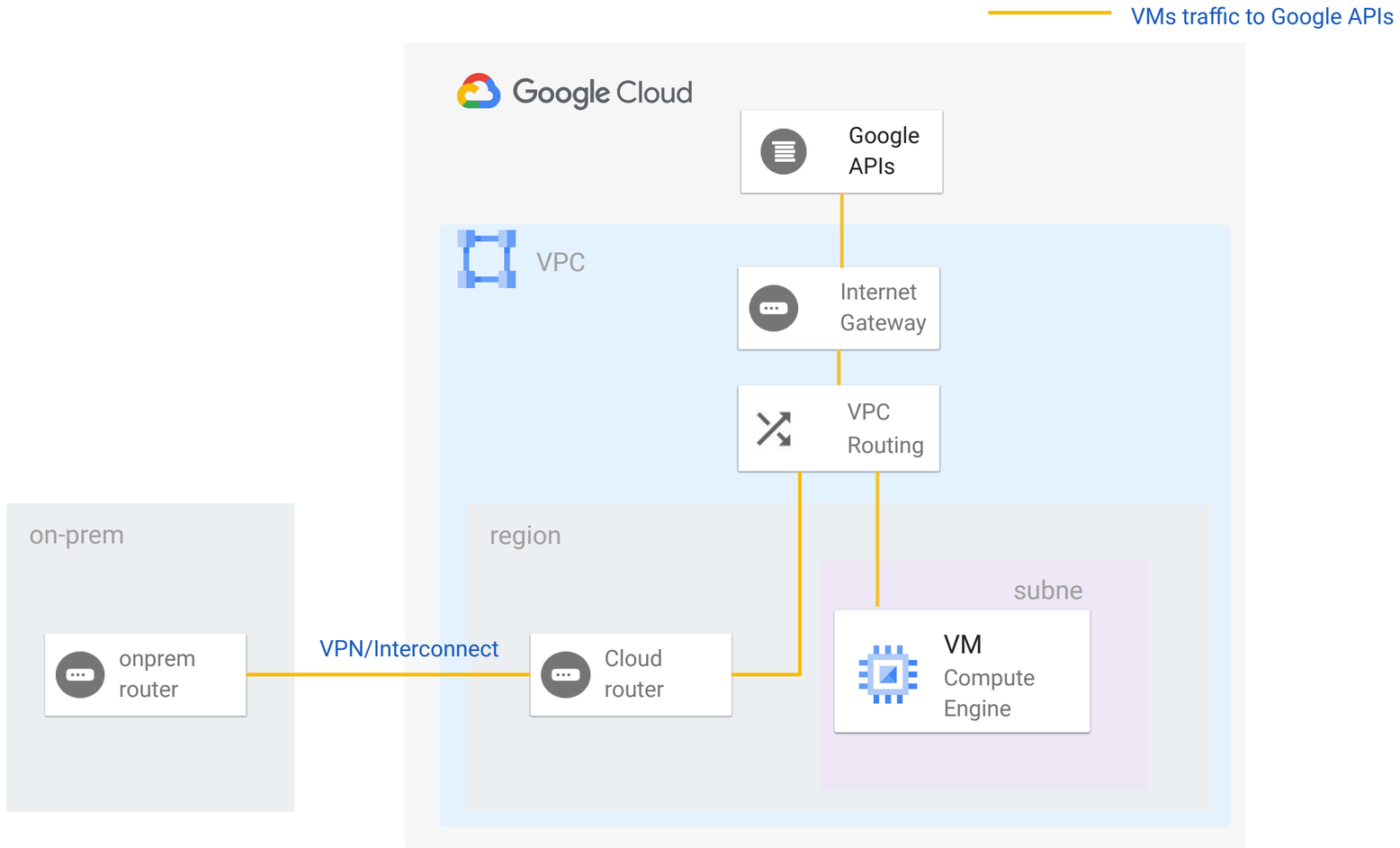
- Google Cloud Storage
- Big Query
- Pub/Sub
- …

Private Google access for on-premises

Private Google Access for on-premises hosts

On-premises hosts can reach Google APIs and services over a Cloud VPN or Cloud Interconnect connection from your data center to Google Cloud.

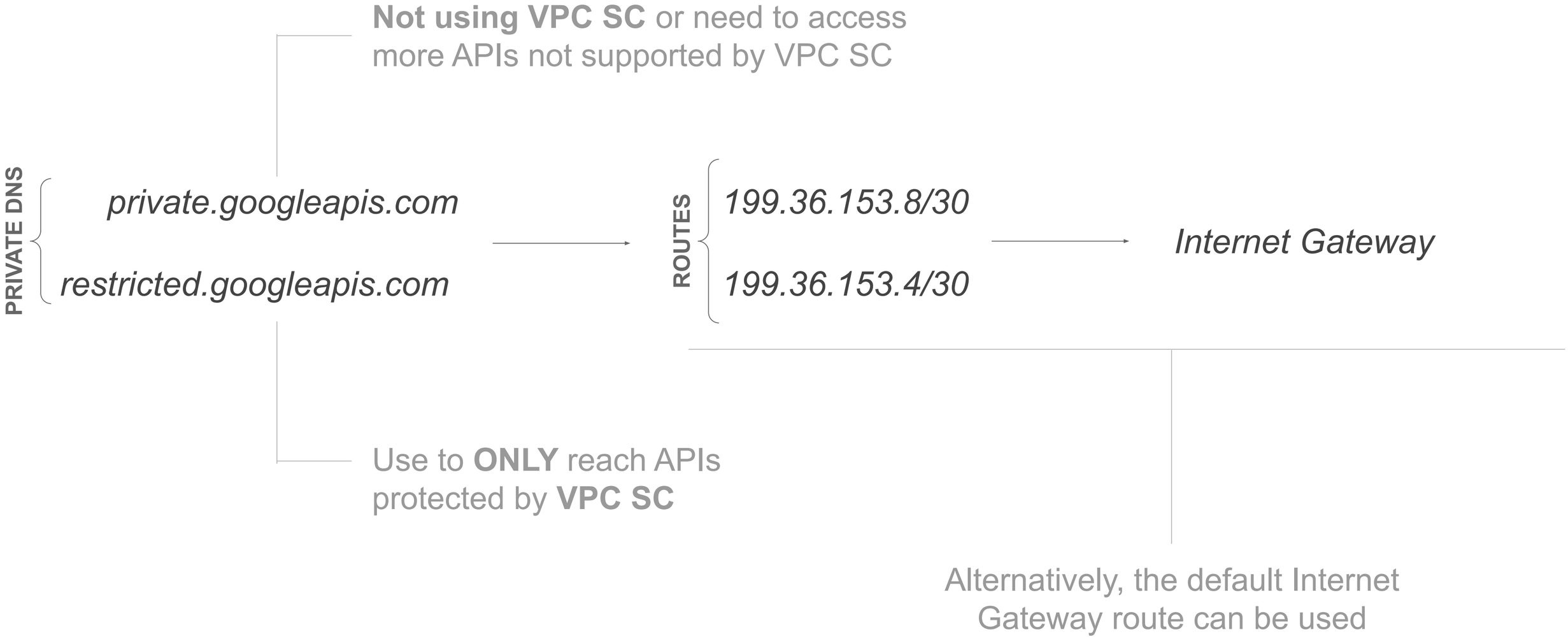
The configuration uses DNS overrides to send API traffic to specific VIPs.



https://cloud.google.com/vpc/docs/private-access-options#pga

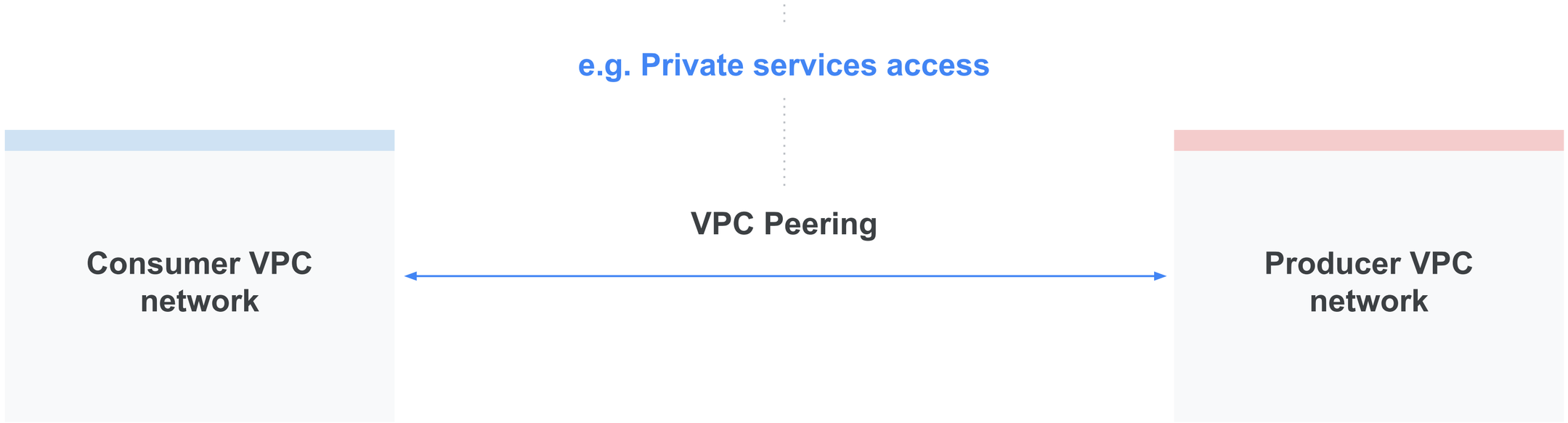
Internal API endpoints for on-prem

(or VPCs without a default route to the Internet Gateway)



Typical Consumer/Producer Networking Setup

- Operational burden, i.e. IP address coordination to avoid overlap between VPCs
- Developers constrained by networking requirements
- Different models for different services, i.e. Private Google Access vs Private services access
- VPC Peering considerations, i.e. quotas and limits, non-overlapping CIDRs, no route filtering



Private Service Access (PSA)

Allows Google Cloud VMs and on-prem networks to access Google Managed Services

Problem:

Instances or on-prem hosts need to reach Google Services deployed in a Google managed VPC

Solution:

Enable **Private Service Access** in the VPC to create a VPC Peering to the Google managed VPC.

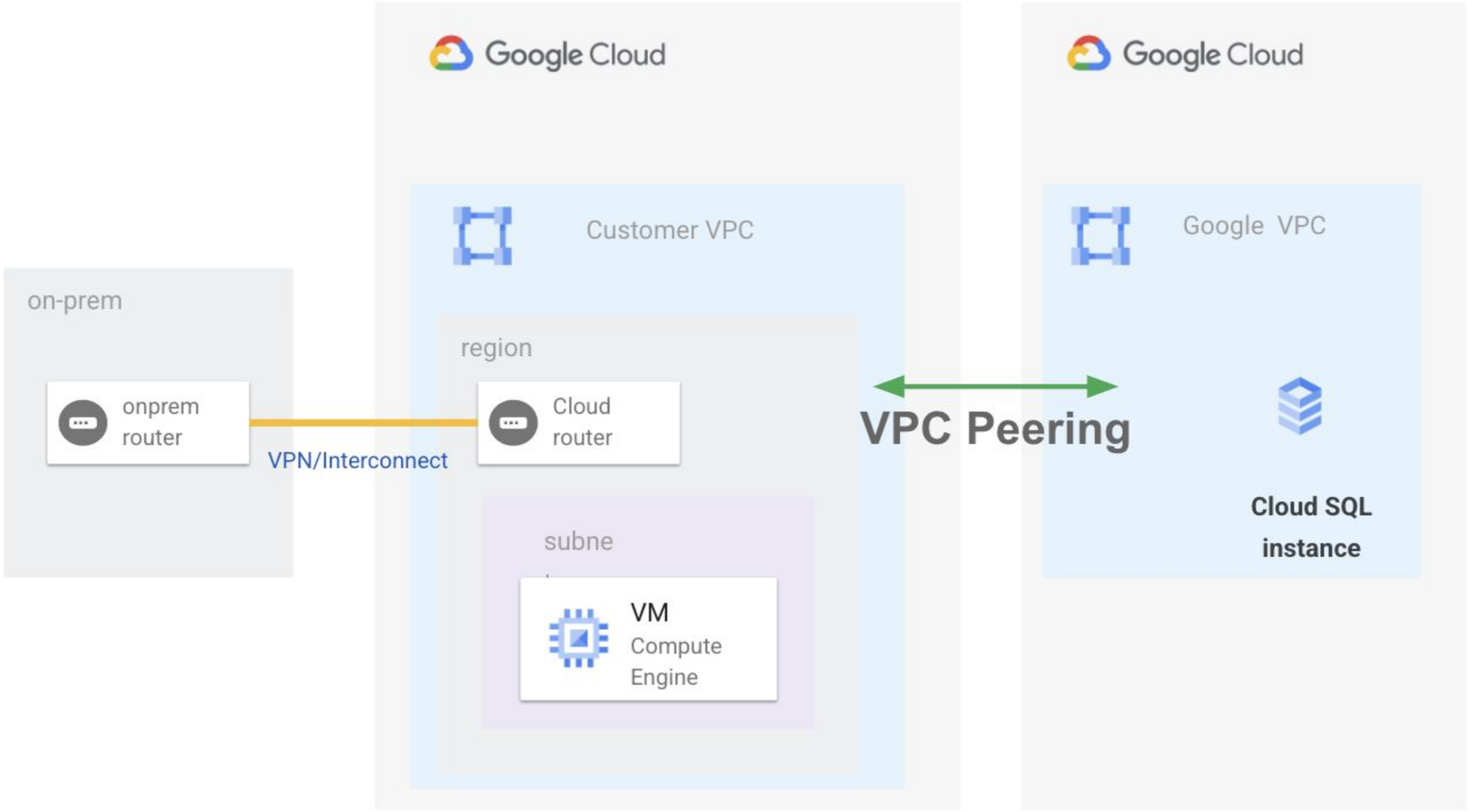
Example of PSA based managed services:

- Cloud SQL
- Memcache
- Cloud IDS
- …

Private Service Access (PSA)

Private Service Access for on-premises hosts

Google Cloud and On-premises hosts (via hybrid connectivity) can reach certain Google managed services over shared VPC peerings.



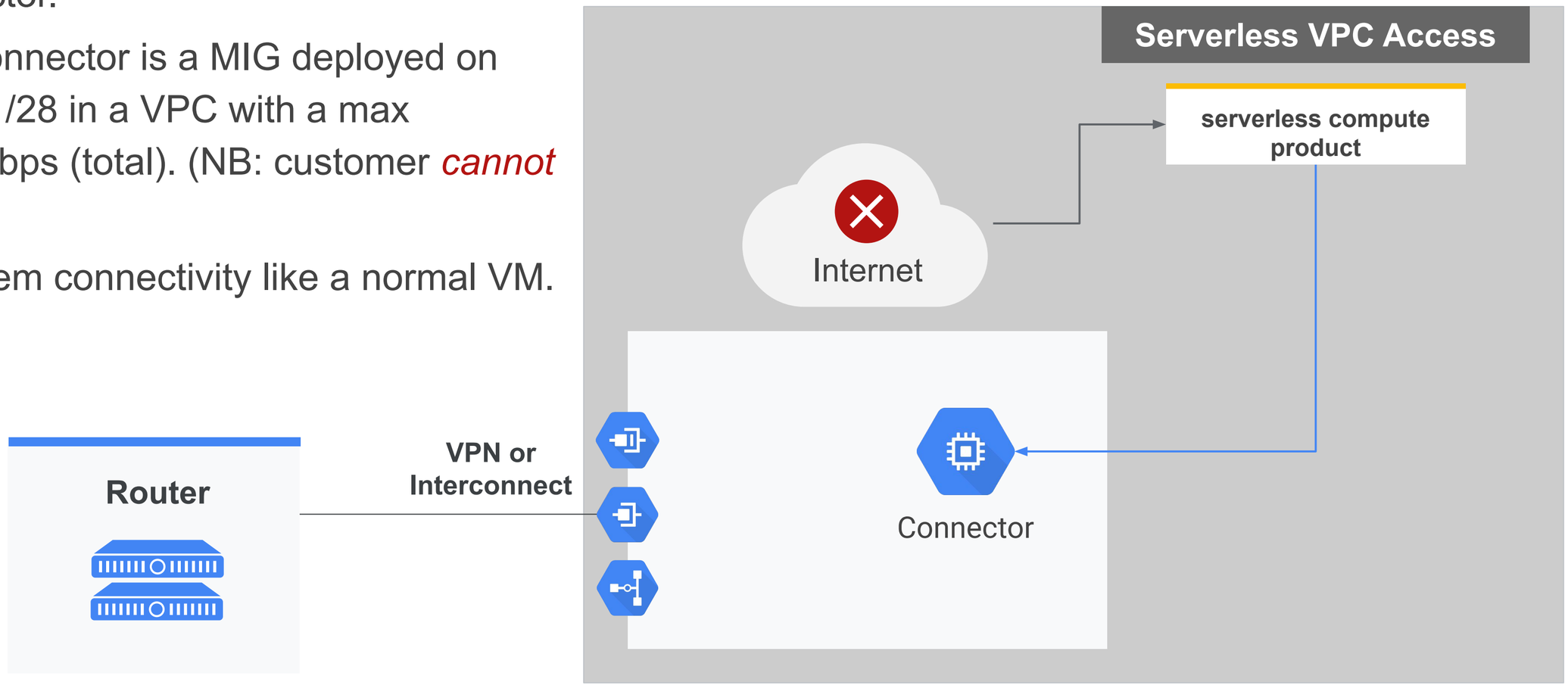
Serverless VPC Access

Cloud Function, Cloud Run, AppEngine standard

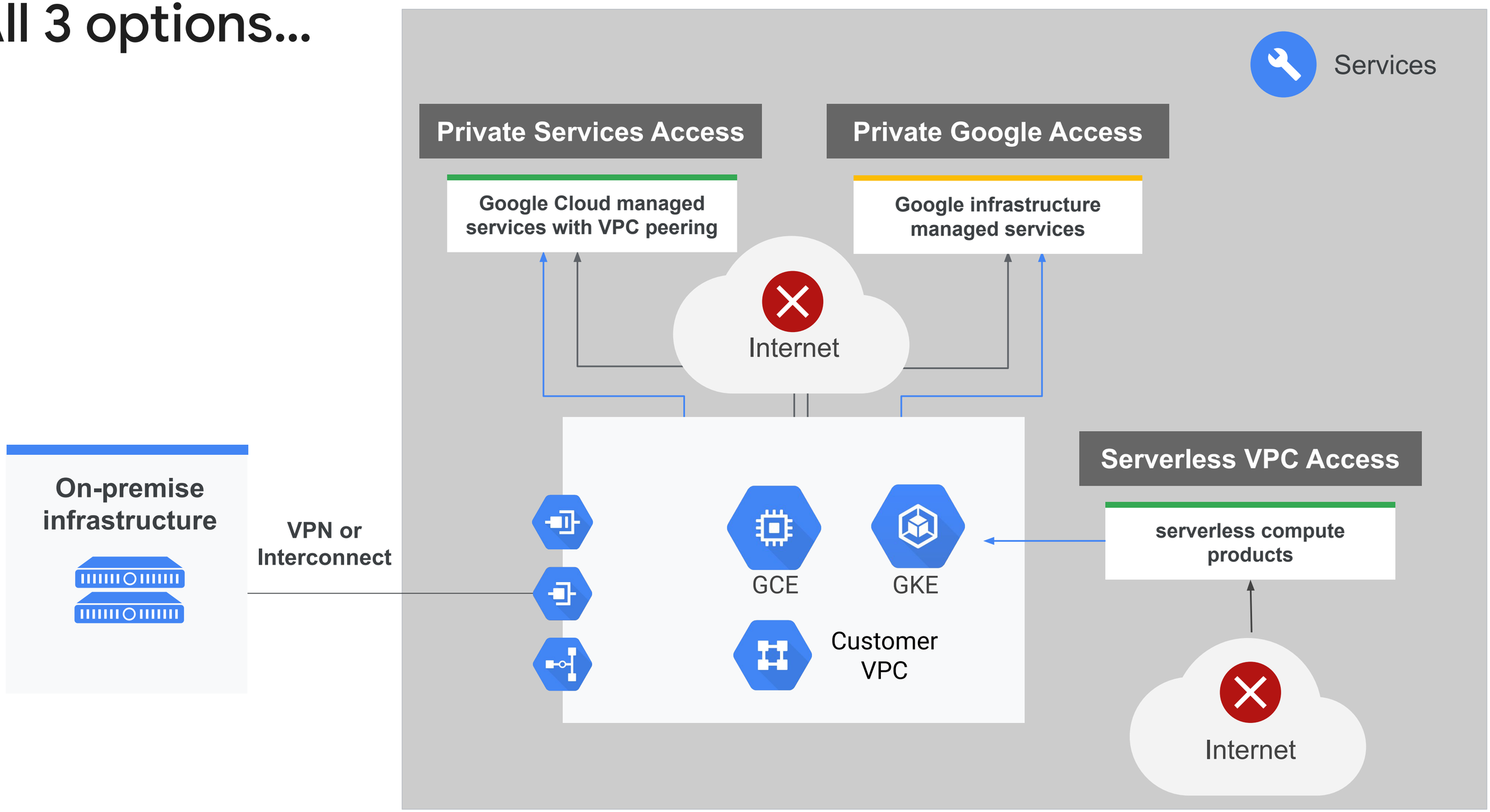
Traffic *initiated* from serverless product is routed through the connector.

Under the hood, connector is a MIG deployed on customer-provided /28 in a VPC with a max throughput of ~1 Gbps (total). (NB: customer *cannot* see MIG today)

Internet and On-prem connectivity like a normal VM.

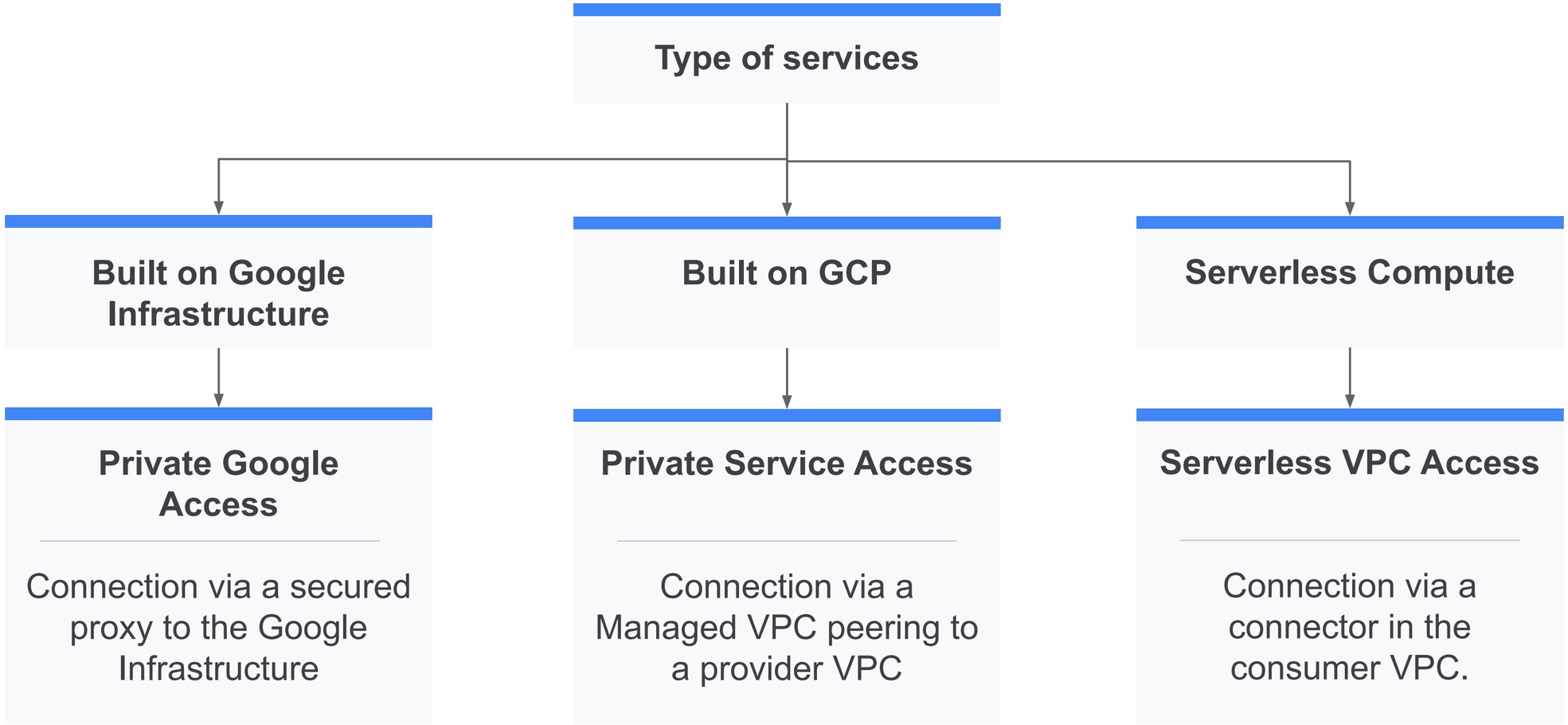


All 3 options...



Solutions Summary

Full list of services:https://cloud.google.com/vpc/docs/private-access-options



A new solution to simplify this area: Private Service Connect

Why Private Service Connect

Consume Services Faster

- Consumer and Producers operate independently
- Support for Single-Tenant and Multi-Tenant Services

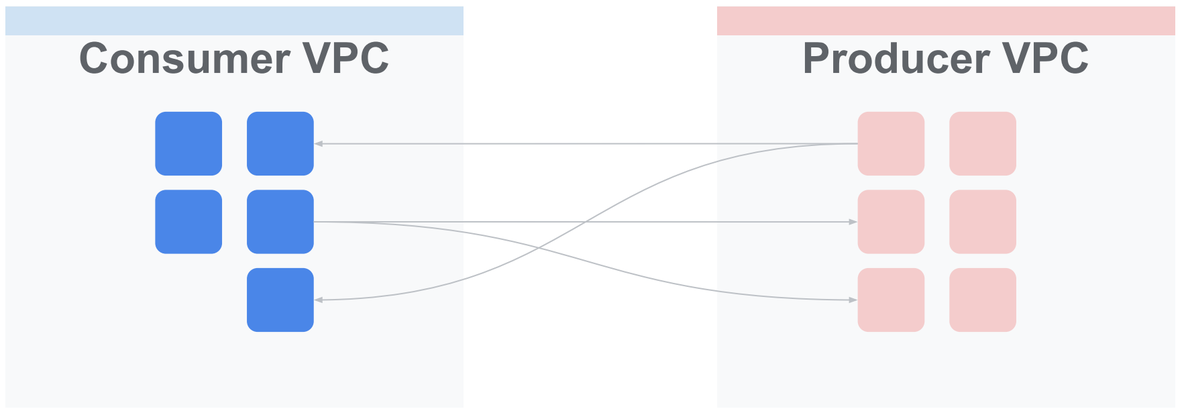
Private and Seamless Connectivity

- Private End to End Connectivity
- Create an Endpoint on the Consumer Network

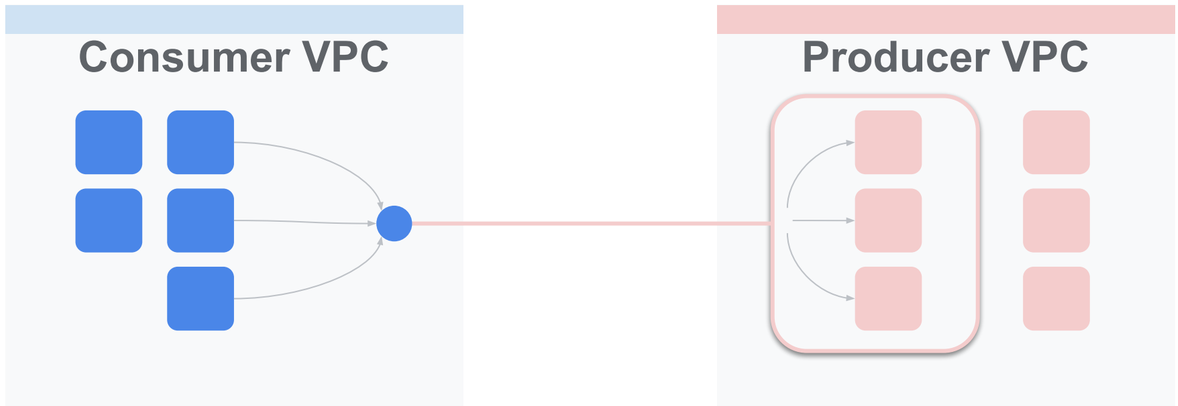
Accelerate Cloud Consumptions

- 1st Party, 3rd Party and Customer Owned Services

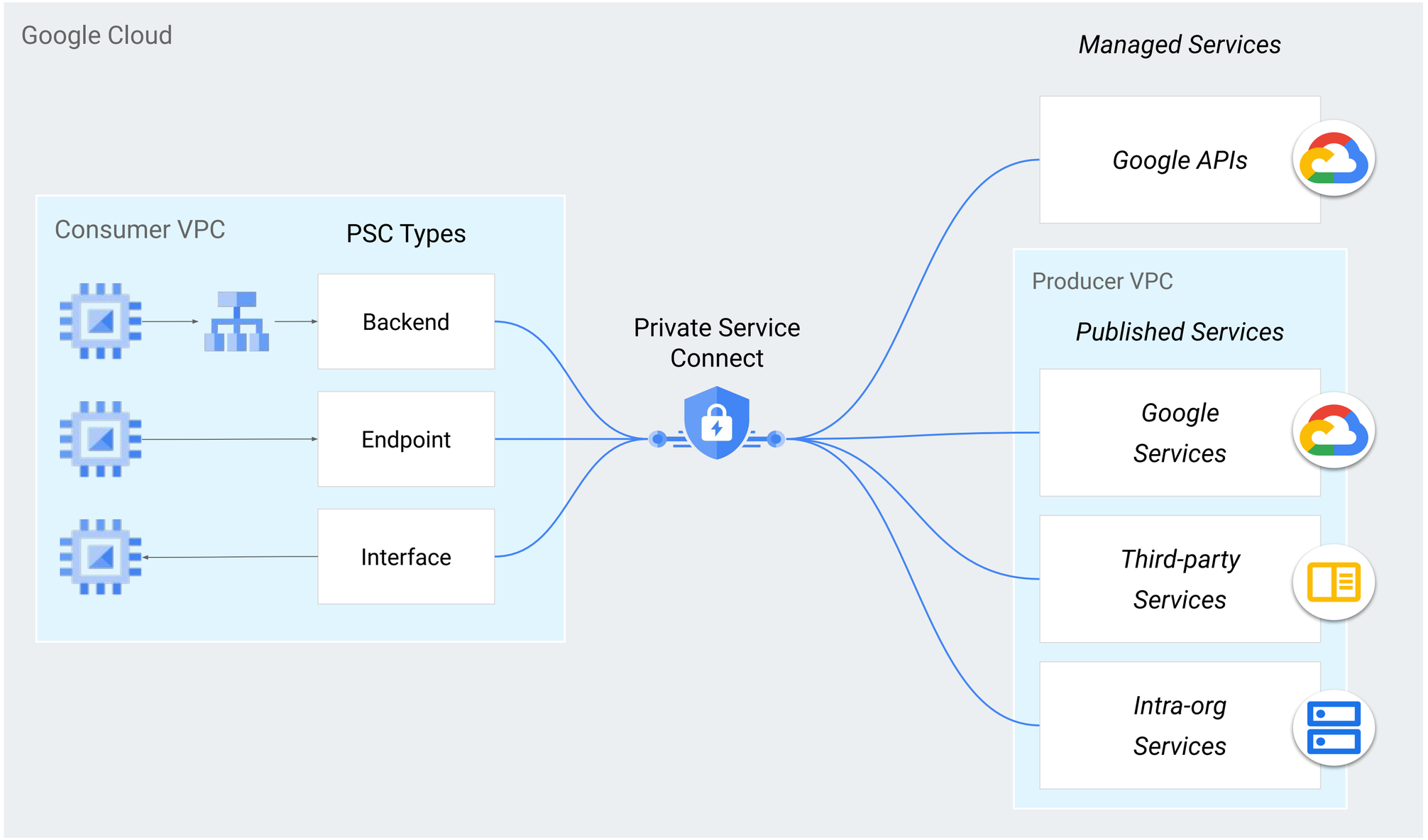
VPC Peering (Private Service Access)



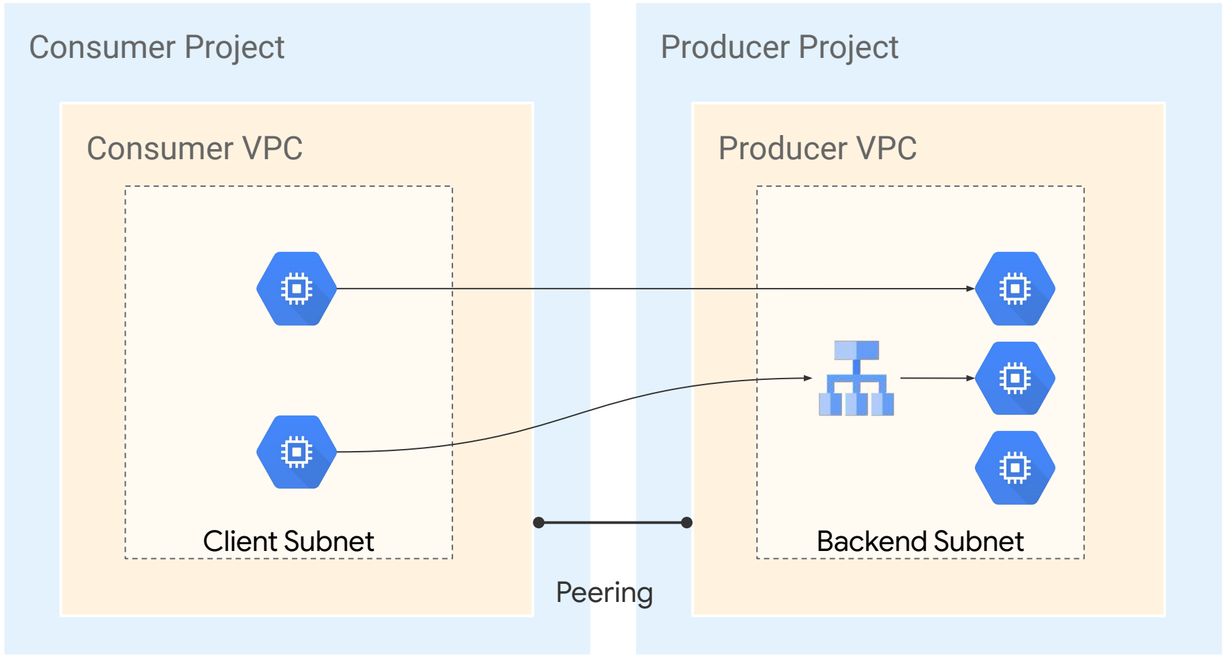
Private Service Connect



PSC for ...


Google Cloud
Managed Services
Google APIs
Consumer VPC
PSC Types
Backend
Endpoint
Interface
Private Service Connect
Producer VPC
Published Services
Google Services
Third-party Services
Intra-org Services

VPC Peering vs Private Service Connect (PSC)

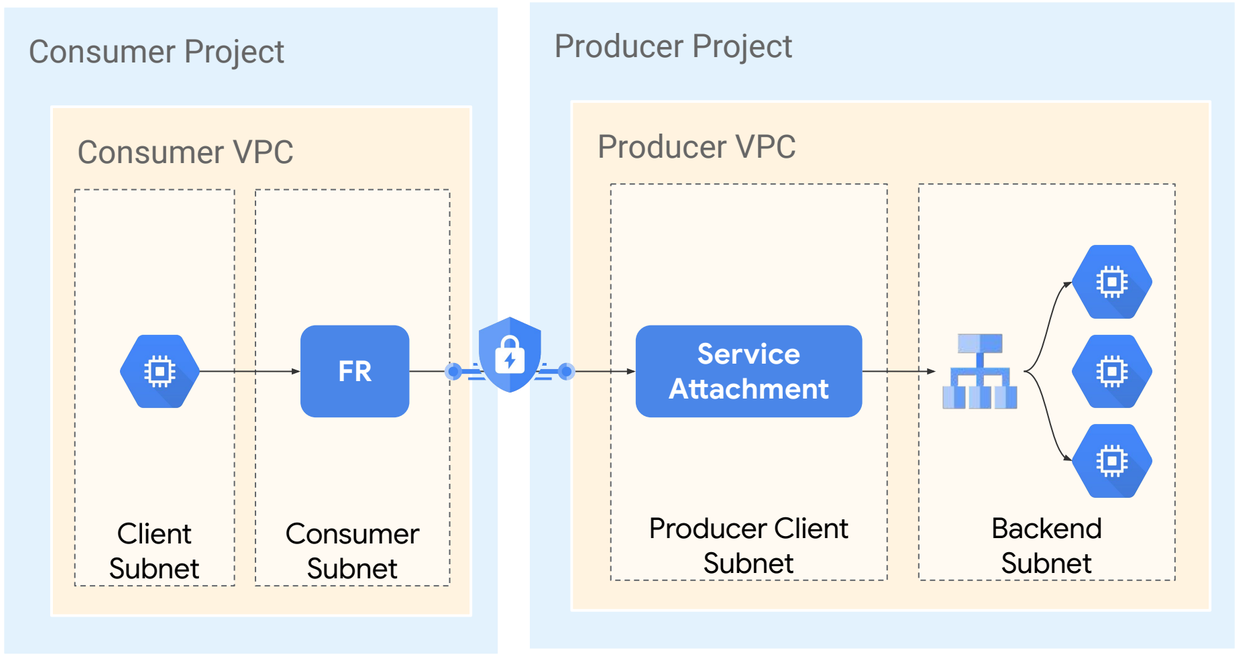


VPC Peering

- Connectivity **between networks**
- **Many-to-many** connectivity
- Constraints
  - Peering group limit
  - No IP subnet overlap

Private Service Connect

- Connectivity from networks **to services**
- **Many-to-one** connectivity
- Constraints
  - No interconnect support (Q3 preview)
  - No multi-regional support (Q3 preview)



Services supported by PSC

Google service	Access provided
Apigee	Lets you expose APIs managed by Apigee to the internet. Also lets you connect privately from Apigee to backend target services.
BeyondCorp Enterprise	Lets the Identity-Aware Proxy access the App Connector Gateway.
Cloud Data Fusion	Lets you connect Cloud Data Fusion instances to resources in VPC networks.
Cloud Composer 2	Lets you access the Cloud Composer tenant project.
Cloud SQL	Lets you access your Cloud SQL database privately.
Cloud Workstations	Lets you access private workstation clusters.
Database Migration Service	Lets you migrate your data to Google Cloud.
Dataproc Metastore	Lets you access Dataproc Metastore services.
Eventarc	Lets you receive events from Eventarc.
Google Kubernetes Engine (GKE) public clusters and private clusters	Lets you privately connect nodes and the control plane for a public or private cluster.
Integration Connectors	Lets Integration Connectors access your managed services privately.
Memorystore for Redis Cluster	Lets you access Memorystore for Redis Cluster instances.
Vertex AI Vector Search	Provides private access to Vector Search endpoints.

2.3 Diagnostic Question 9 Discussion

An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Use a Cloud VPN tunnel. Use your DNS provider to create DNS zones and records for private.googleapis.com. Connect the DNS provider to your on-premises network. Broadcast the request from the on-premises environment. Use a software-defined firewall to manage incoming and outgoing requests.

B. Use Partner Interconnect. Configure an encrypted tunnel in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and A records for private.googleapis.com.

C. Use a Cloud VPN tunnel. Use Cloud DNS to create DNS zones and records for *.googleapis.com. Set up on-premises routing with Cloud Router. Use Cloud Router custom route advertisements to announce routes for Google Cloud destinations.

D. Use Direct Interconnect. Configure a VLAN in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and records for restricted.googleapis.com and private.googleapis.com. Set up on-premises routing with Cloud Router. Add custom static routes in the VPC to connect individually to BigQuery, Cloud Storage, and Compute Engine instances.

2.3 Diagnostic Question 9 Discussion

An external audit agency needs to perform a one-time review of Cymbal Bank's Google Cloud usage. The auditors should be able to access a Default VPC containing BigQuery, Cloud Storage, and Compute Engine instances where all the usage information is stored. You have been tasked with enabling the access from their on-premises environment, which already has a configured VPN.

What should you do?

A. Use a Cloud VPN tunnel. Use your DNS provider to create DNS zones and records for private.googleapis.com. Connect the DNS provider to your on-premises network. Broadcast the request from the on-premises environment. Use a software-defined firewall to manage incoming and outgoing requests.

B. Use Partner Interconnect. Configure an encrypted tunnel in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and A records for private.googleapis.com.

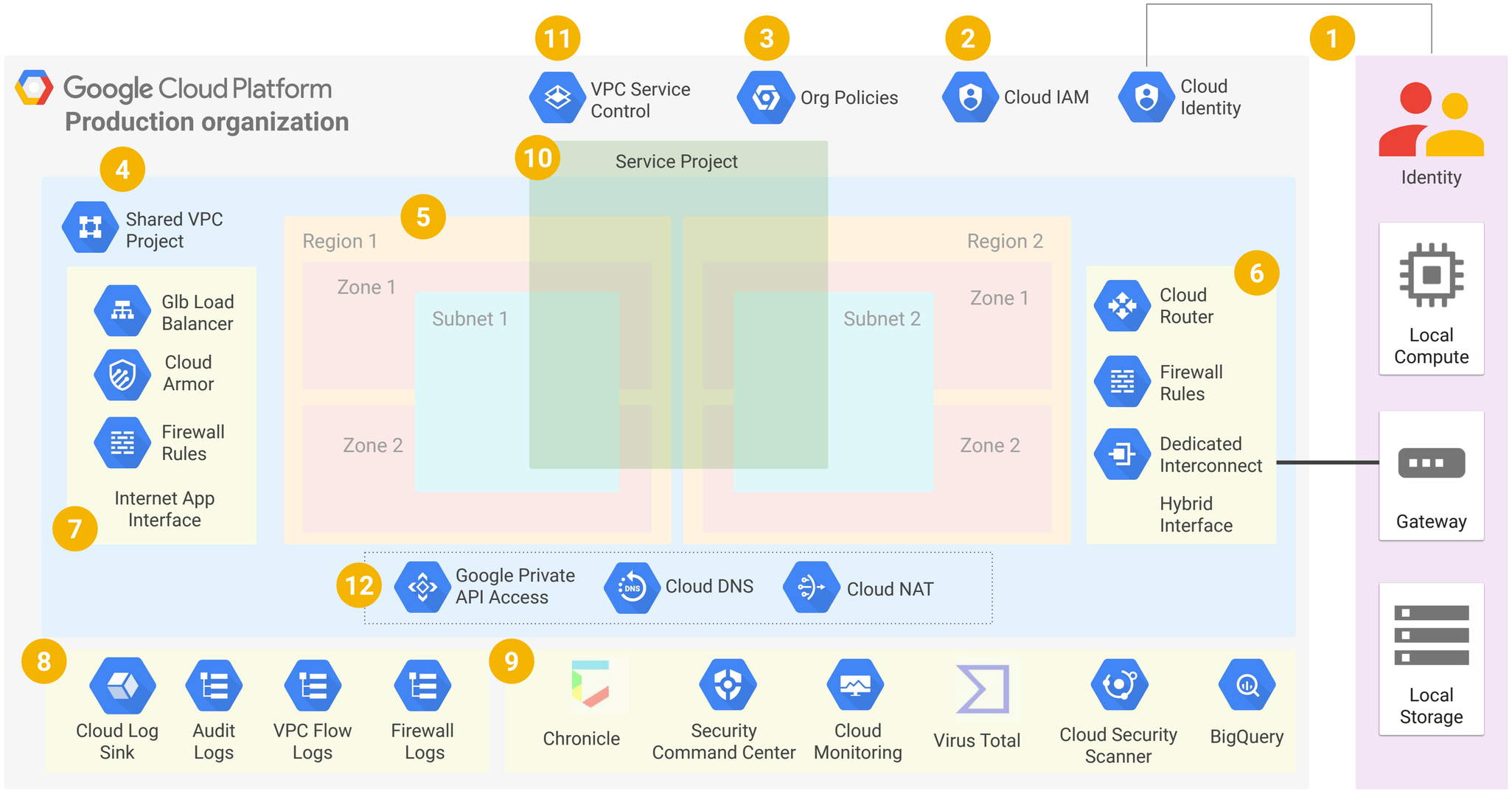
C. Use a Cloud VPN tunnel. Use Cloud DNS to create DNS zones and records for *.googleapis.com. Set up on-premises routing with Cloud Router. Use Cloud Router custom route advertisements to announce routes for Google Cloud destinations.

D. Use Direct Interconnect. Configure a VLAN in the auditor's on-premises environment. Use Cloud DNS to create DNS zones and records for restricted.googleapis.com and private.googleapis.com. Set up on-premises routing with Cloud Router. Add custom static routes in the VPC to connect individually to BigQuery, Cloud Storage, and Compute Engine instances.

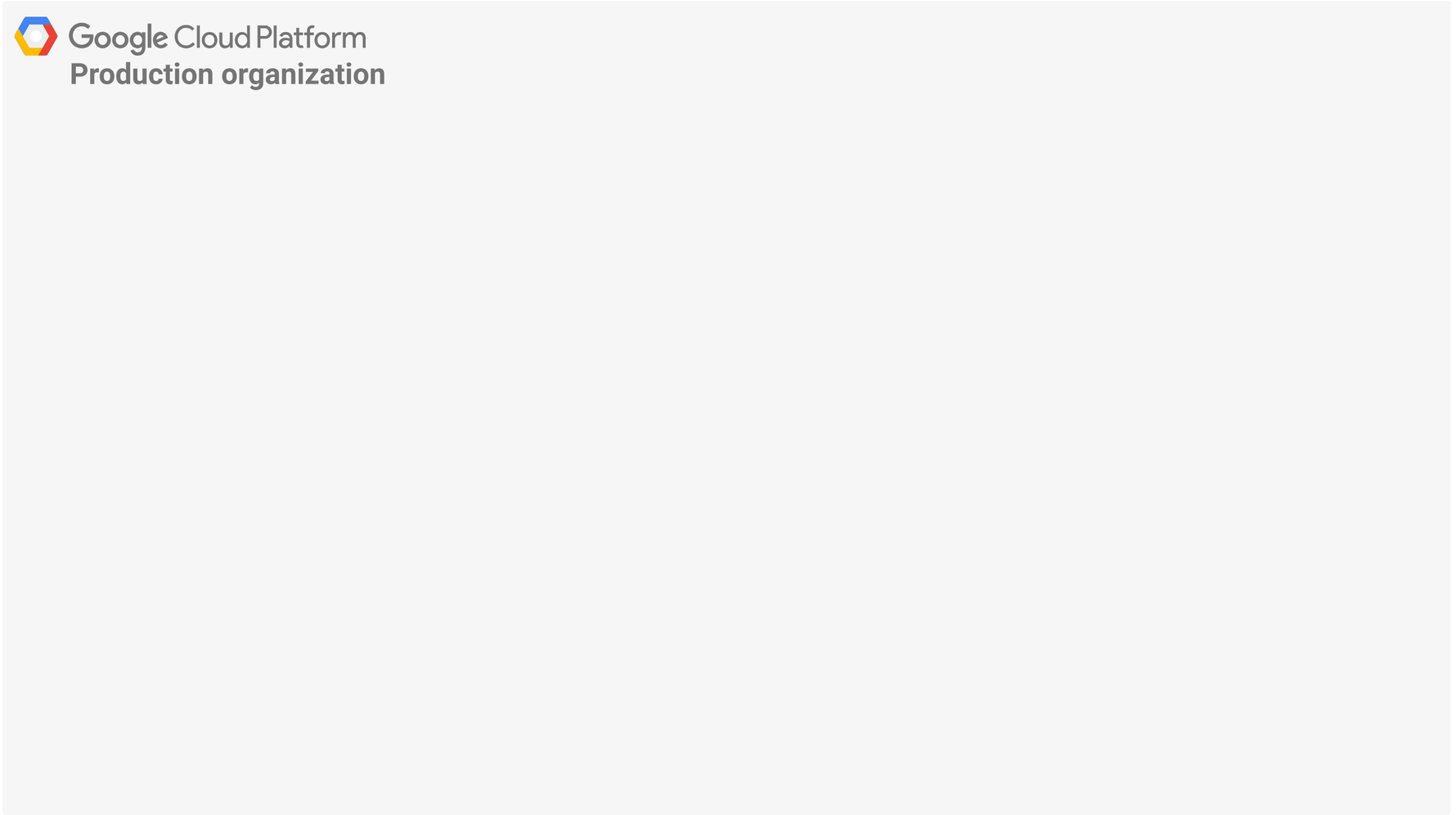
Security Foundations Blueprint

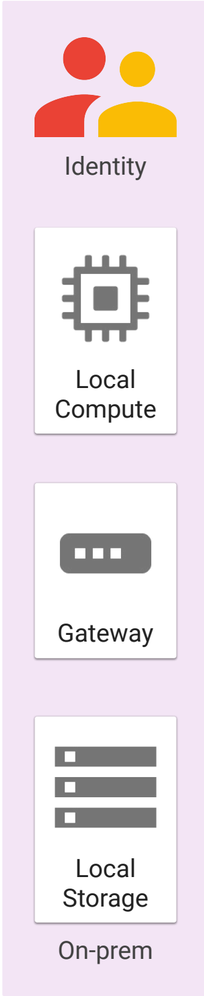
Introducing: Security Foundations Blueprint

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Cloud Logging Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. Create a service project to host workloads
11. Create security perimeter with VPC-SC
12. Access GCP services and the Internet through private IP



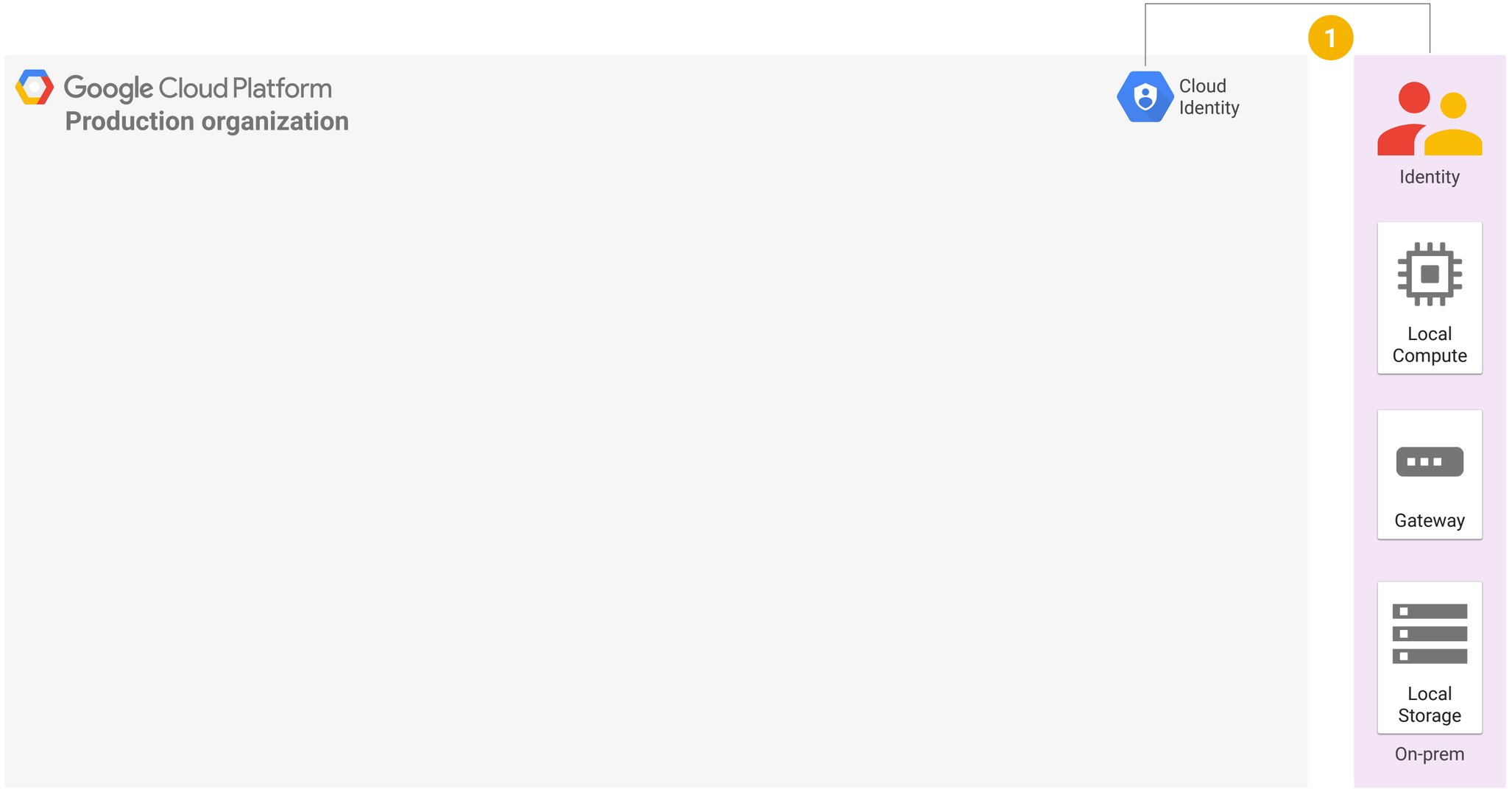
Foundation blueprint: Start





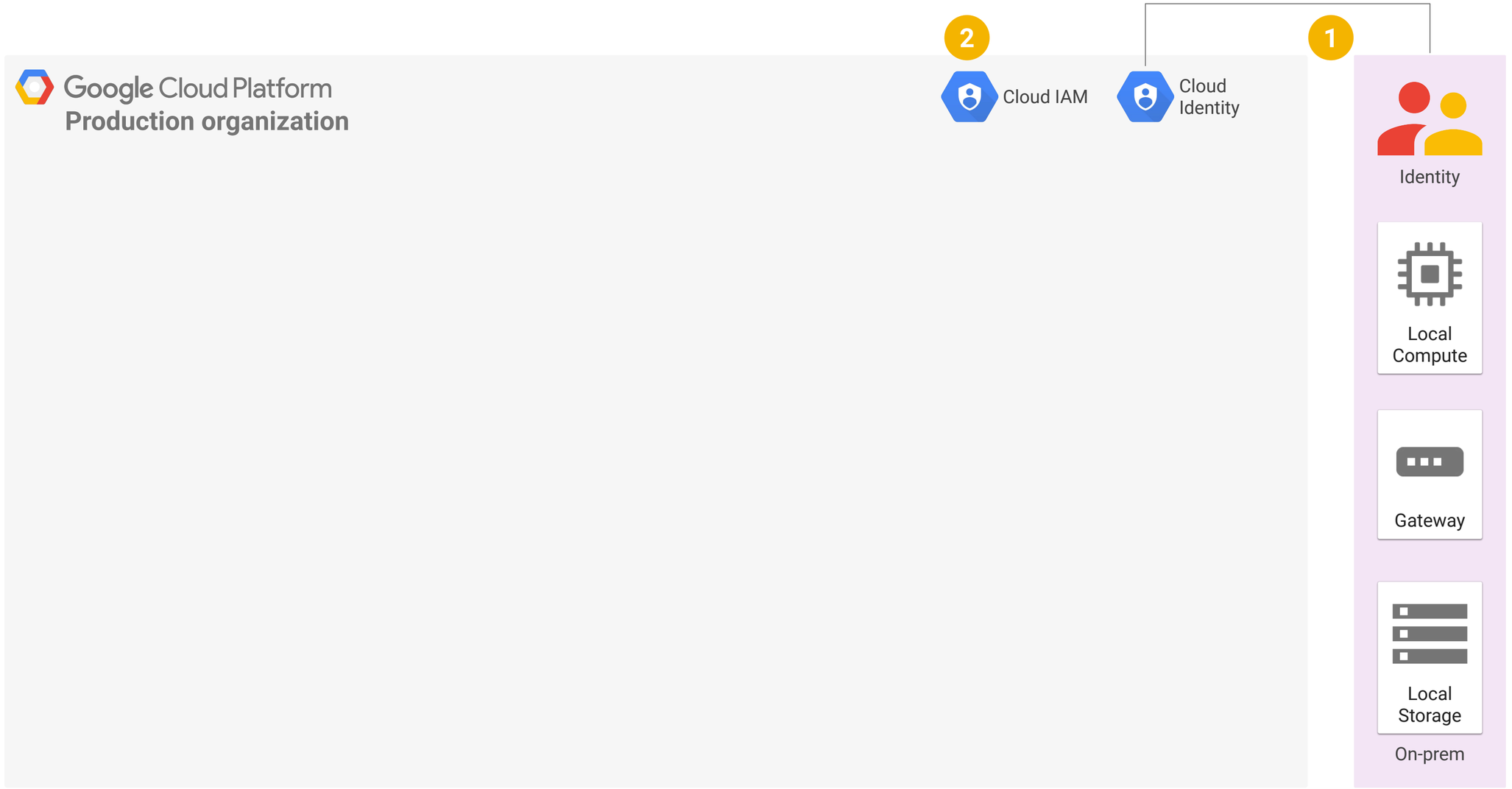
Foundation blueprint: Step 1

1. **Establish unified Identity with on-prem**



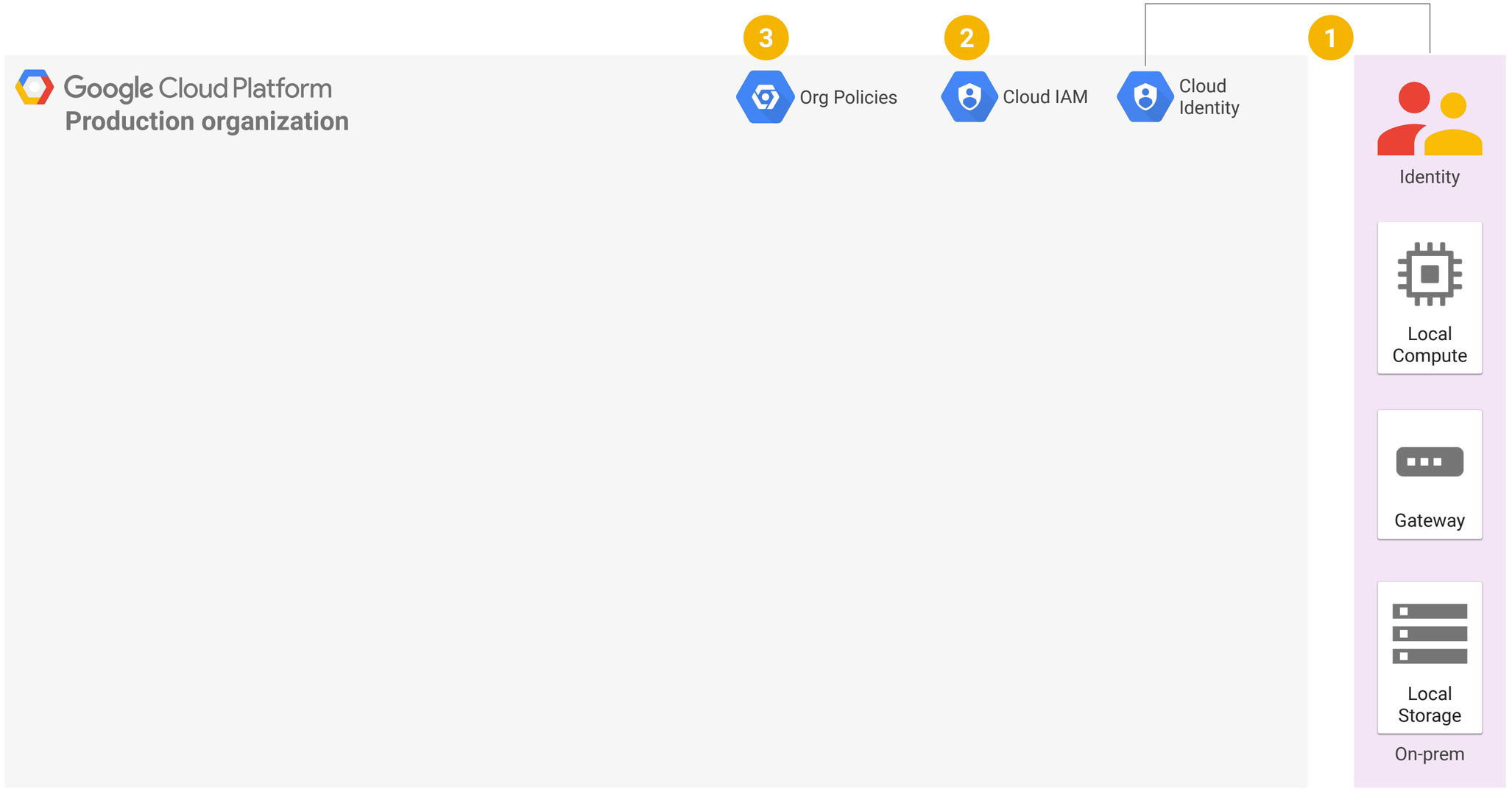
Foundation blueprint: Step 2

1. Establish unified Identity with on-prem
2. **Create roles with least privilege access through IAM**



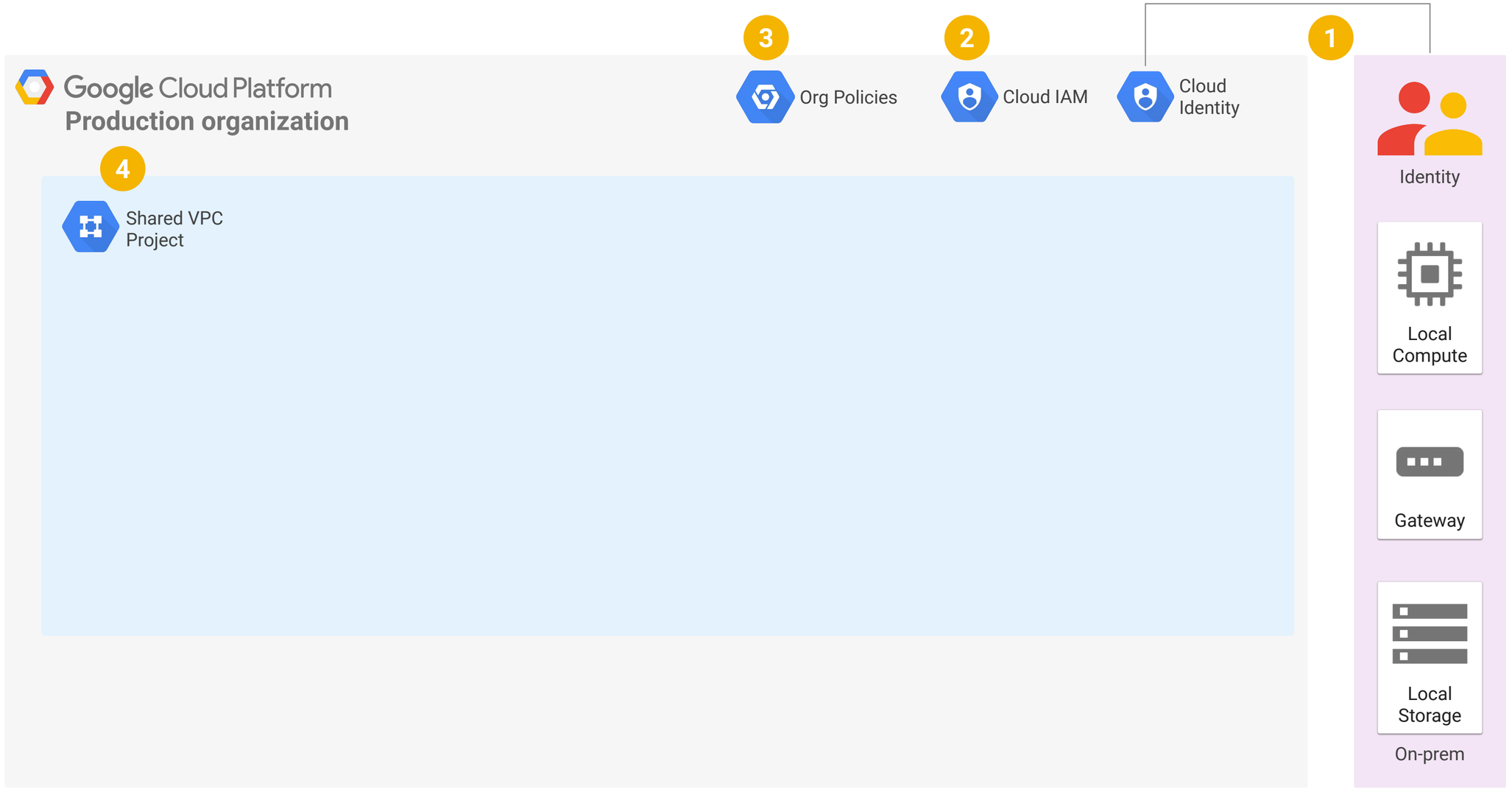
Foundation blueprint: Step 3

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. **Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)**



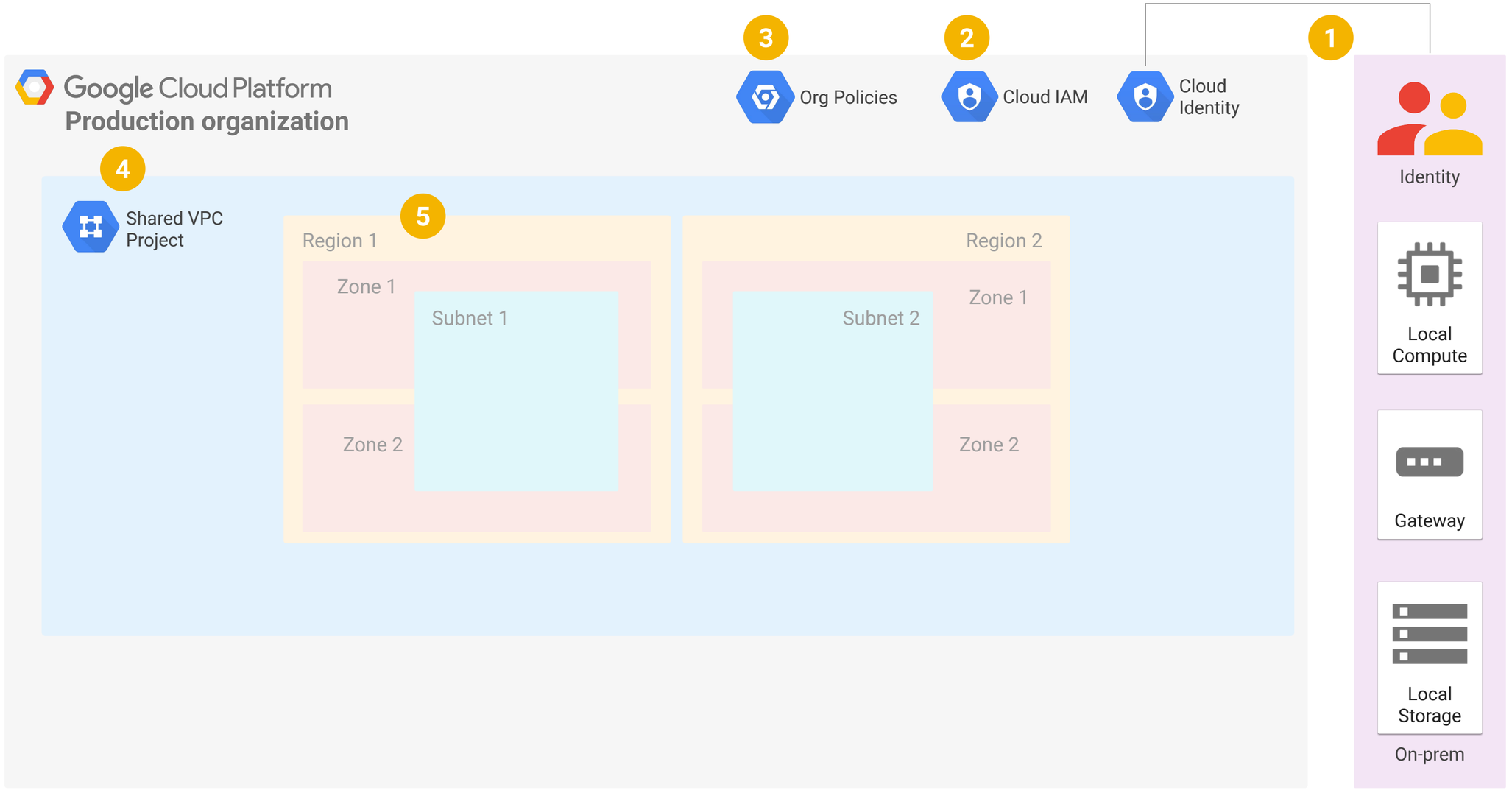
Foundation blueprint: Step 4

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. **Leverage shared VPC for connectivity and segregated network control**



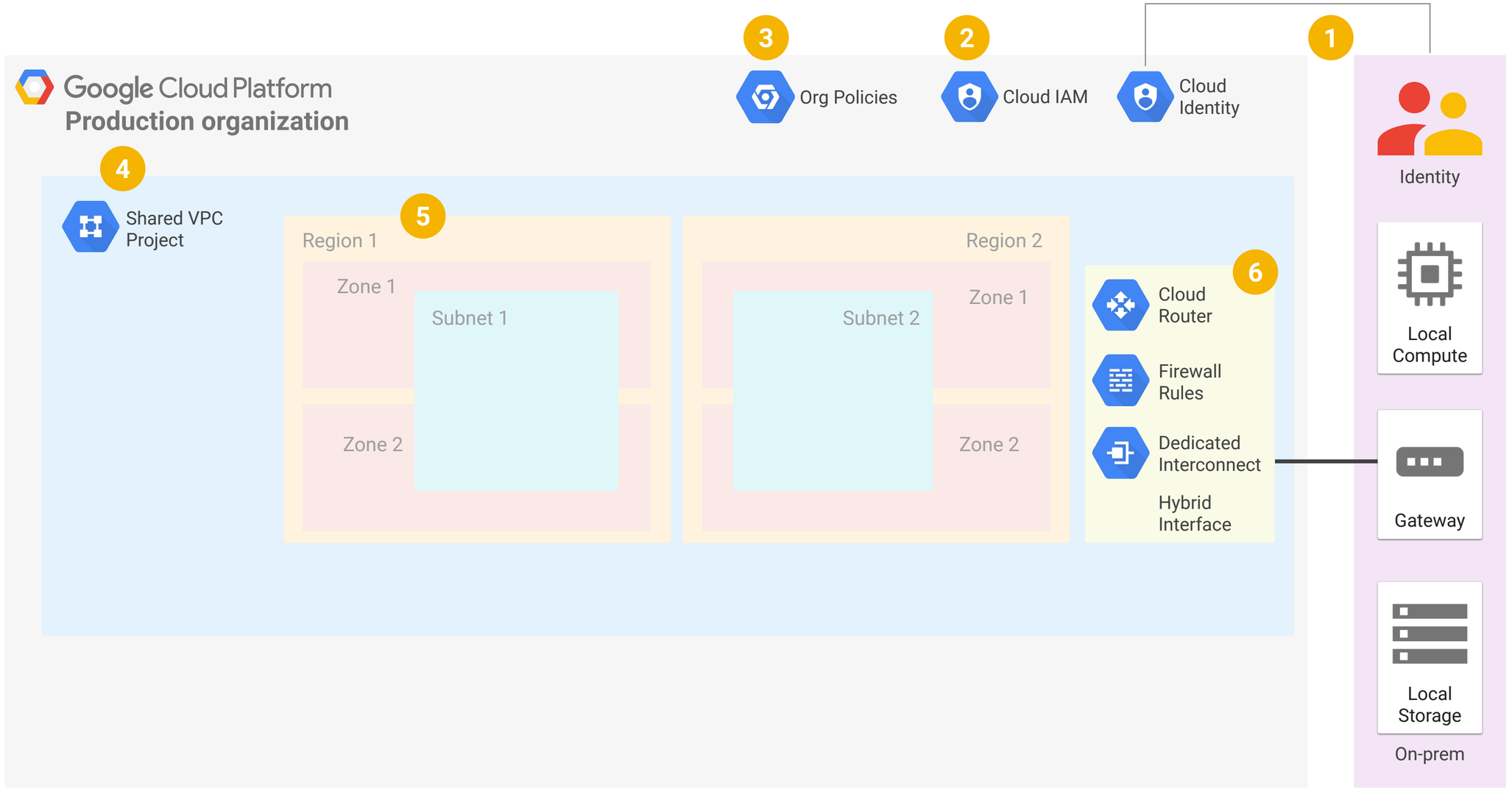
Foundation blueprint: Step 5

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. **Build HA/DR topologies - multi-AZ/multi-region with subnets**



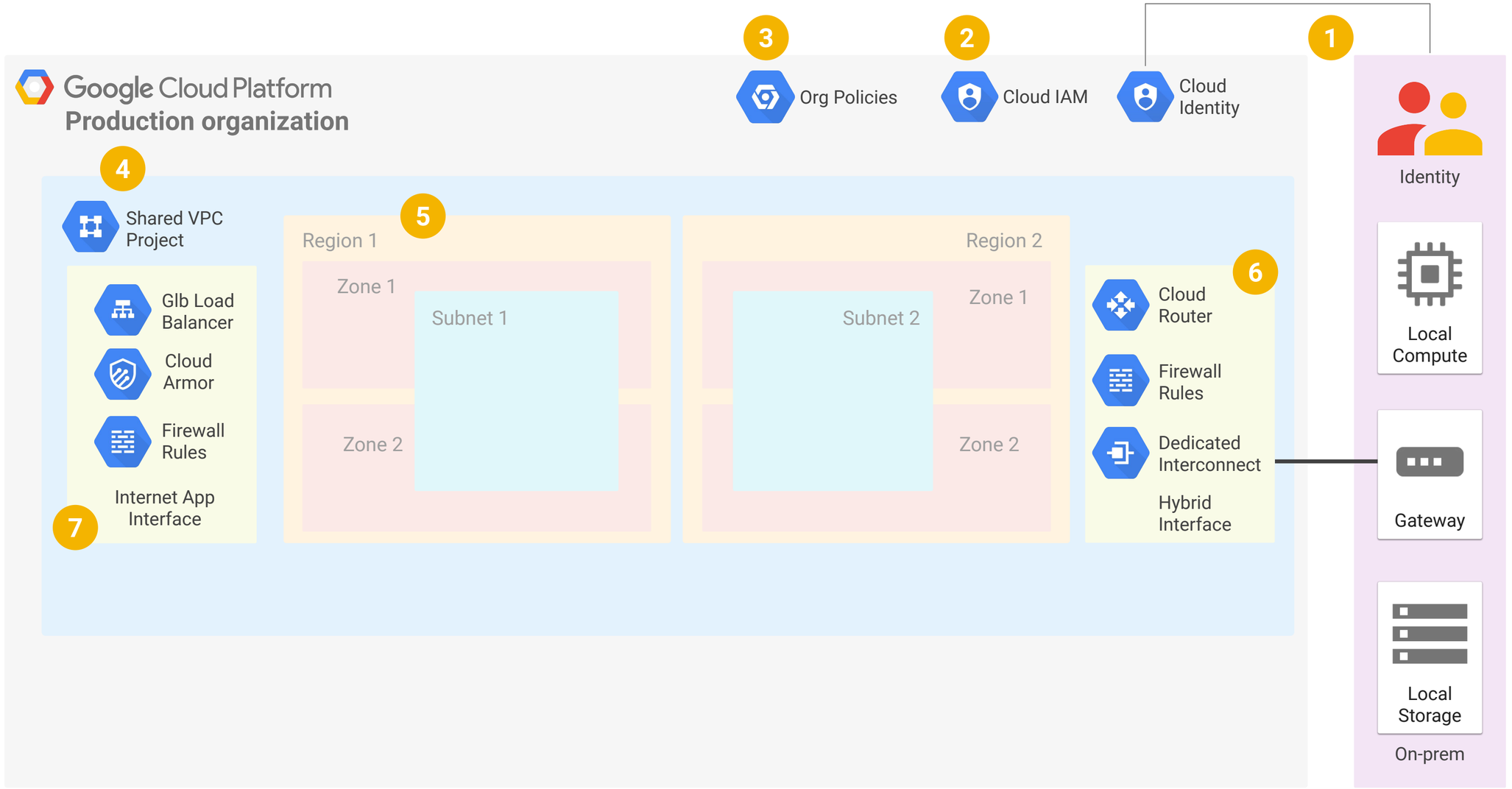
Foundation blueprint: Step 6

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. **Interface to on-prem with Direct Interconnect**



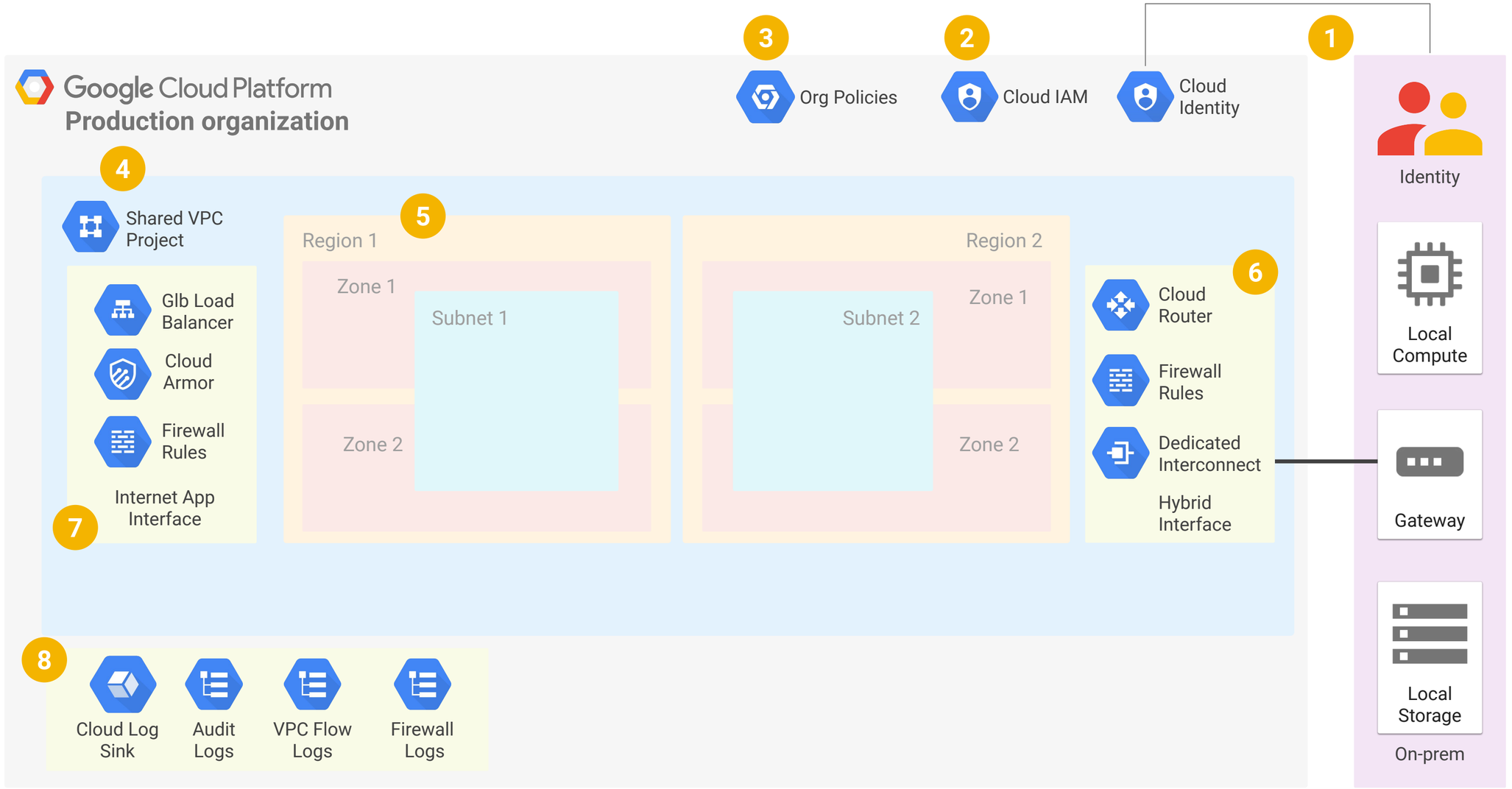
Foundation blueprint: Step 7

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. **Secure App I/F against DDoS and external threats with GLB/CA & Firewalls**



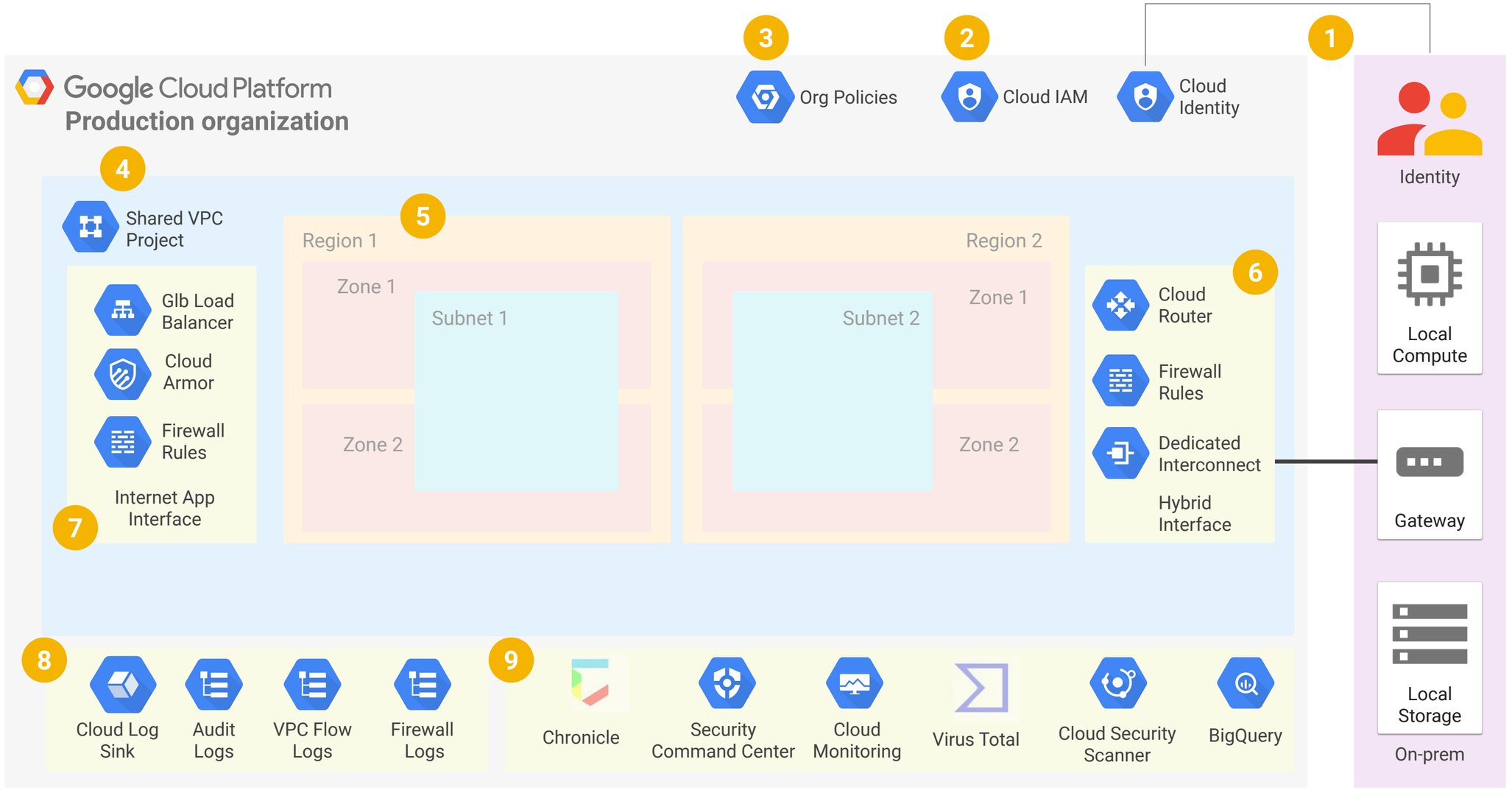
Foundation blueprint: Step 8

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. **Leverage Cloud Logging Log Sink to collect logs**



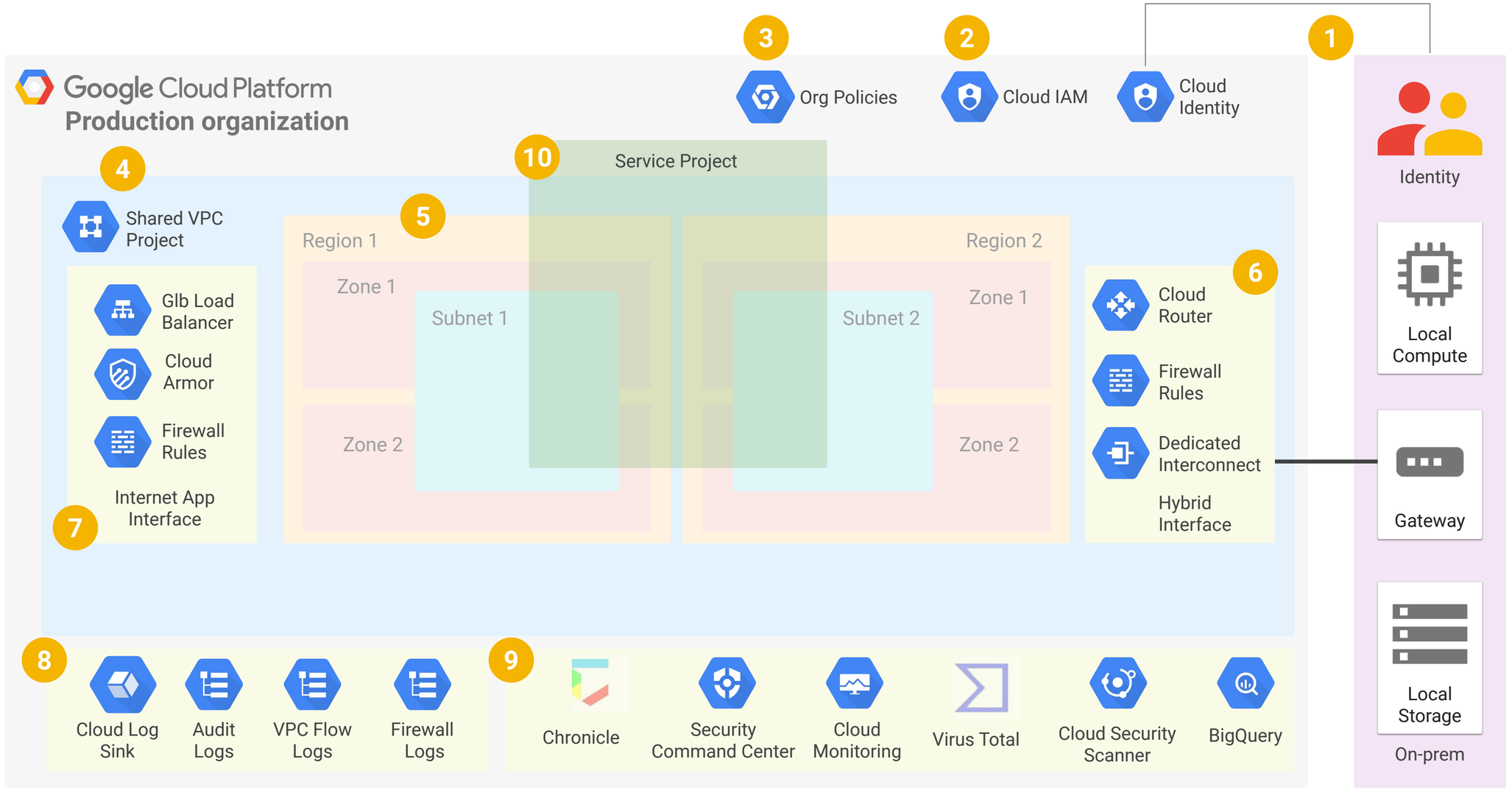
Foundation blueprint: Step 9

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Cloud Logging Log Sink to collect logs
9. **Monitor environment with Cloud Native tools**



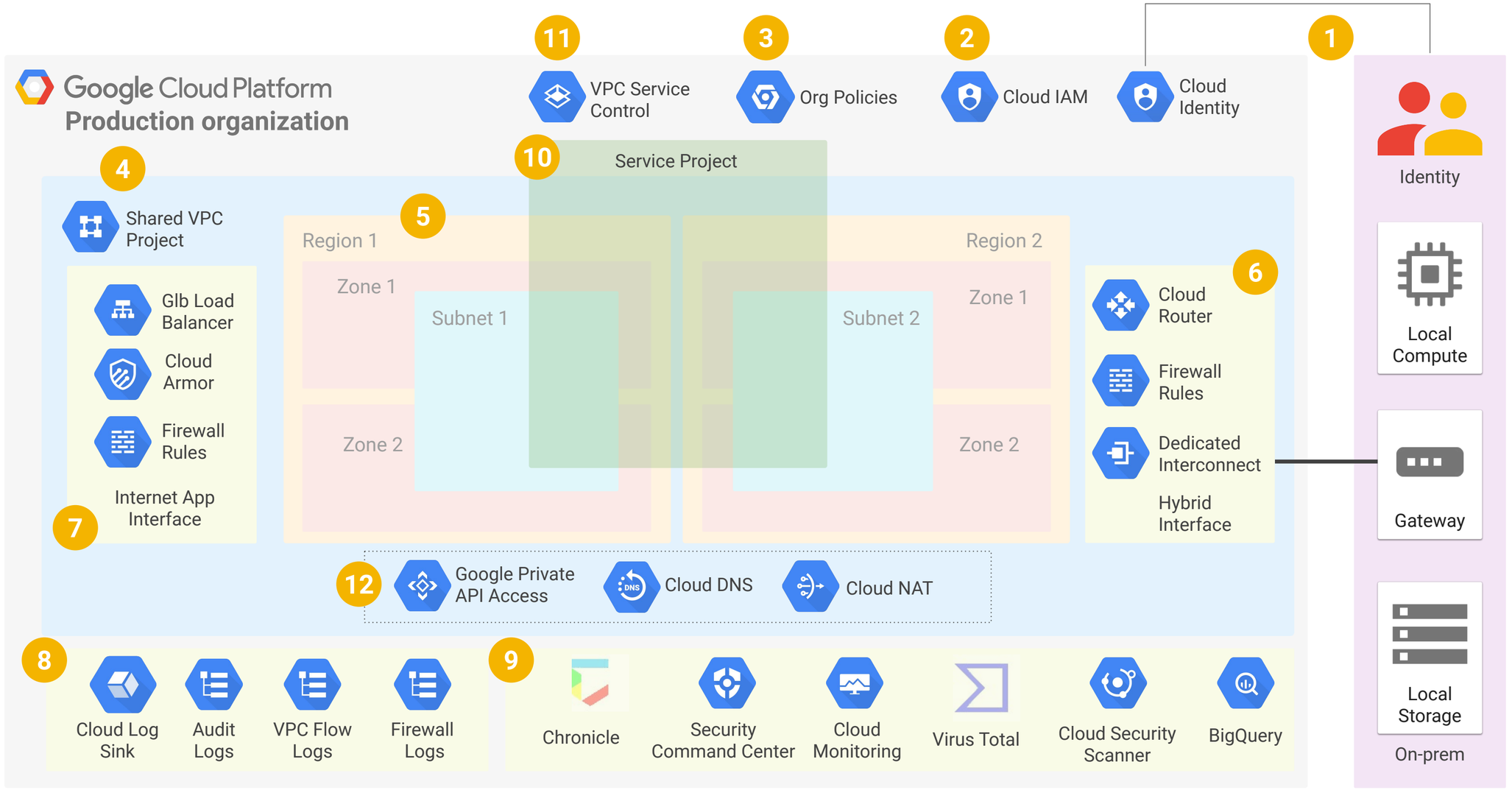
Foundation blueprint: Step 10

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Cloud Clogging Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. **Create a service project to host workloads**



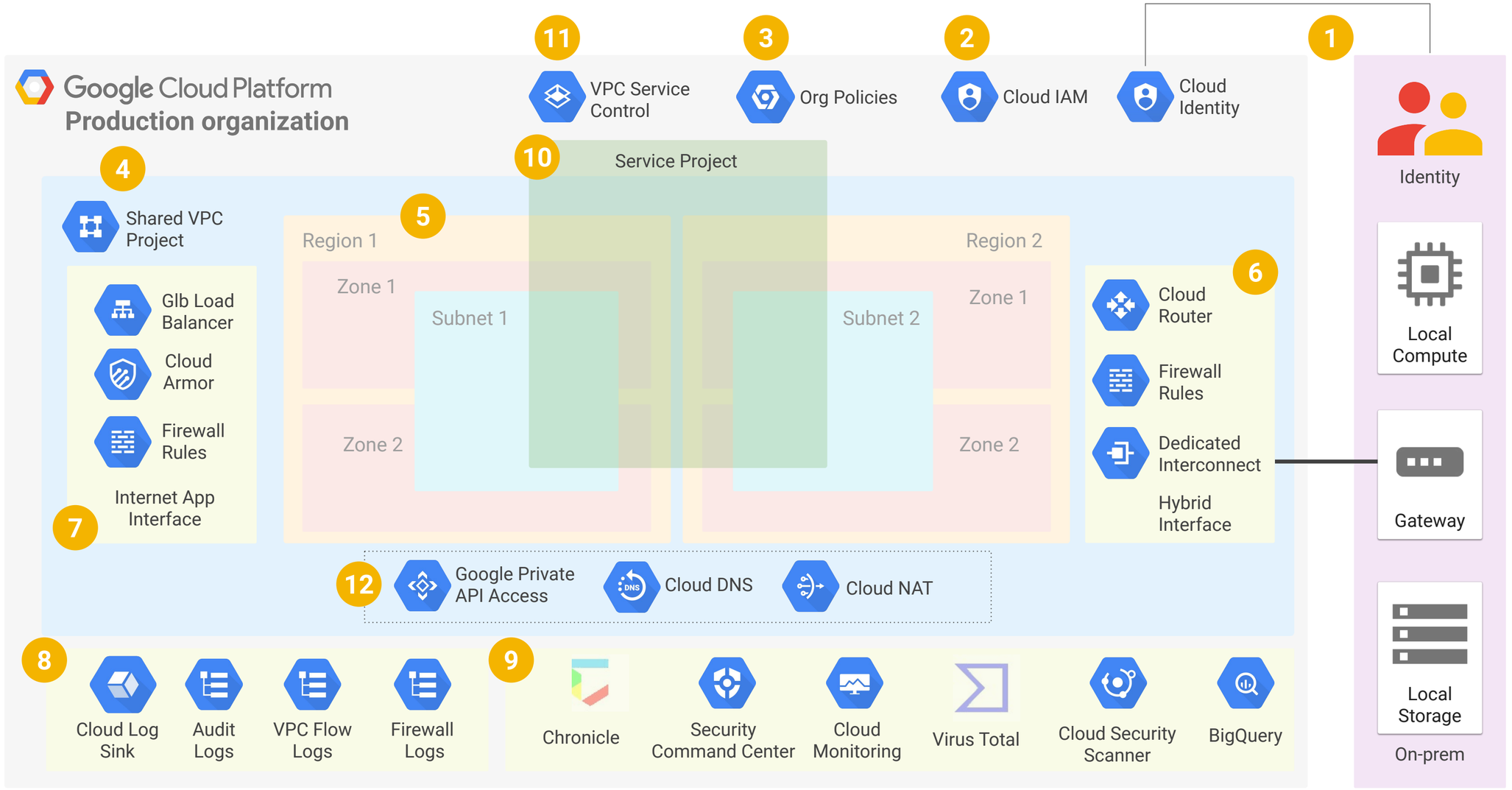
Foundation blueprint: Step 11

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Cloud Logging Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. Create a service project to host workloads
11. **Create security perimeter with VPC-SC**



Foundation blueprint: Step 12

1. Establish unified Identity with on-prem
2. Create roles with least privilege access through IAM
3. Establish Org level policies (no external IPs, Domain Restricted Sharing, Trusted Images)
4. Leverage shared VPC for connectivity and segregated network control
5. Build HA/DR topologies - multi-AZ/multi-region with subnets
6. Interface to on-prem with Direct Interconnect
7. Secure App I/F against DDoS and external threats with GLB/CA & Firewalls
8. Leverage Cloud Logging Log Sink to collect logs
9. Monitor environment with Cloud Native tools
10. Create a service project to host workloads
11. Create security perimeter with VPC-SC
12. **Access GCP services and the Internet through private IP**



Bonus content

Very subjective way to evaluate if you're ready…

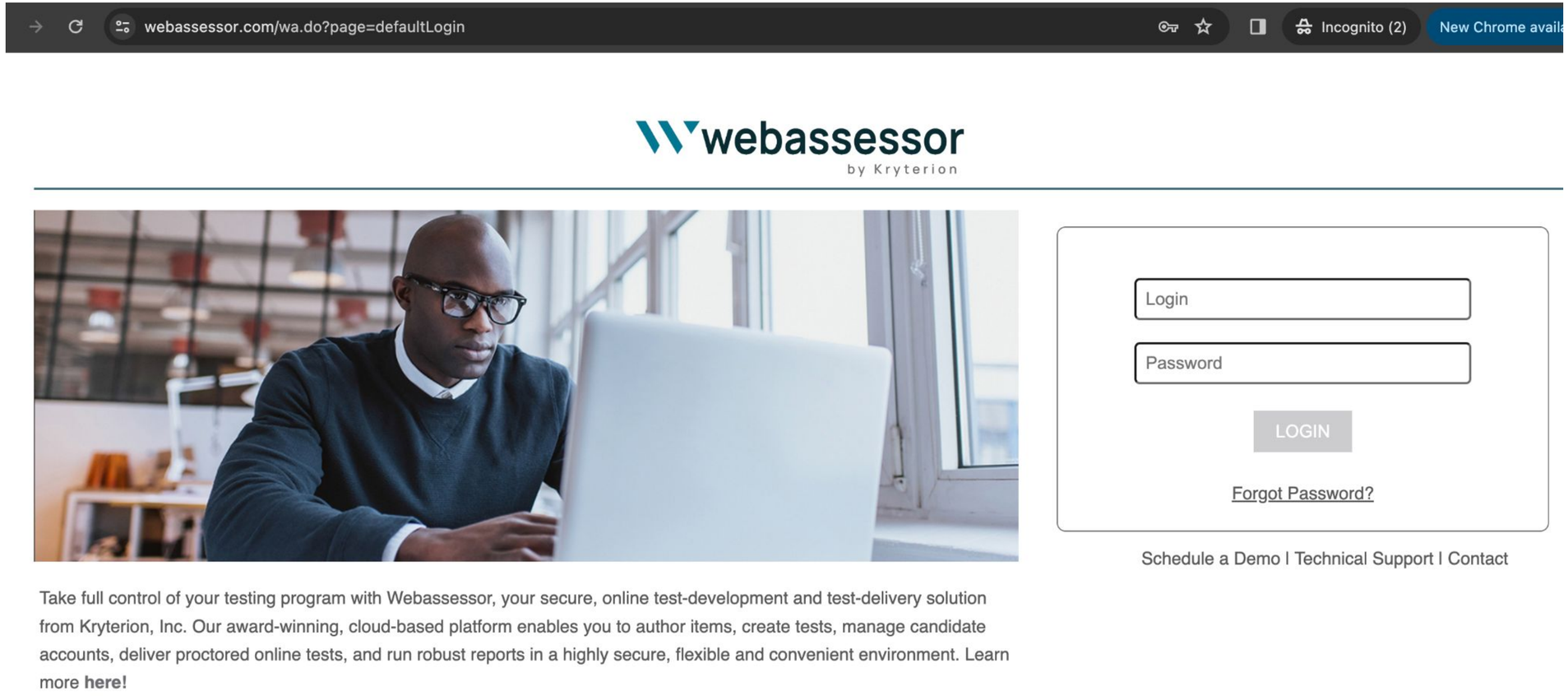
0: not covered on the exam at all	**Professional Cloud Security Engineer (PCSE)**	0: none
1: basics (high-level functionality and use-cases)		1: basics
2: medium (1 + prerequisites, limitations, common IAM roles, ability to integrate with other services, most common architectures)		2: medium
3: advanced (2 + being able to deploy, troubleshoot and manage)		3: advanced
4: expert (3 + know every detail about the service in complex configurations - huge scale, HA, DR etc)		4: expert

		Recommended minimum knowldege level for PCA	My knowledge level (self-assesment)
Security and Identity			
	Binary Authorization	2: medium	0: none
	Cloud Asset Inventory	2: medium	0: none
	Cloud Data Loss Prevention	3: advanced	0: none
	Cloud Key Management Service	3: advanced	0: none
	Cloud Security Command Center	2: medium	0: none
	VPC Service Controls	3: advanced	0: none
	Web Security Scanner	2: medium	0: none
	Cloud EKM	2: medium	0: none
	Cloud HSM	2: medium	0: none
	Shielded VMs	1: basics	0: none
	Confidential Computing	1: basics	0: none
	Service Accounts	3: advanced	0: none
	Titan Security Key	1: basics	0: none
	Access Transparency	2: medium	0: none
	Chronicle	1: basics	0: none
	BeyondCorp / BeyonProd model	2: medium	0: none

PCA PCSE

LINK - switch to "PCSE" tab

How to register for the exam?



webassessor.com

Start by creating an account on Certmetrics - new Google Cloud Certification platform

Exam notes & tips

PCSE exam tips&tricks

- know when to use DNSSEC and what it protects against. Link.
- BigQuery - know the options to assign permissions selectively (Authorized View concept, column-level access control, dynamic data masking, row-level access control)
- Know how to redirect specific logs to external SIEM tools. Link. Link2.
- Know how to analyze all traffic using 3rd party threat detection tool (Packet Mirroring, Cloud IDS).
- Know most popular Org Policies; know how they propagate down and how to break this propagarion. Link.
- Restricted.googleapis for accessing VPC Service Controlled GCP services from on-prem. Link.
- Redirect and centralize logging -> log bucket vs GCS bucket, set on org level, Log Router sinks. Link. Link2.
- Know where Cloud Armor can be used (which types of LBs are supported). Link.
- How to prepare to move projects between organizations (remove VPC Service Controls, deploy target folders for projects to be moved etc). Link.
- How to grant broad IAM privileges to a group of people that can access the service only when something happens (via a separate Service Account and granting Service Account User on this account + IAM Conditions...)

PCSE exam tips&tricks

- How to manage dry-run policies of VPC Service Controls without breaking the current setup.
- Access Context Manager. Link.
- Cloud NAT use-cases
- Which load balancer can be used with Standard Network Tier. Link.
- A lot of questions about managing keys - what if we need to be aligned with GDPR (CMEK), what if FIPS-140 ... (HSM), etc
- Differentiate between Secret Manager and KMS (secrets / keys)
- Quite some details about DLP - what types to use if data needs to be decrypted later on, what to use when we ingest photos containing PII. Link.
- How to ensure data is only stored in a specific region (org-level policies that deny creation of services outside of selected regions, plus VPC-SC).
- What SPECIFIC IAM roles are needed to manage budgets and billing on org level. Link.
- How to prevent developers from creating SA keys (org policy specific for KEYS only, not SAa)
- How to prevent from threats after encryption key is compromised (rotate automatically in regular intervals, plus block suspected ones). Link.
  - Can't auto-rotate asymmetric keys!

PCSE exam tips&tricks

- **How to secure GKE architecture**
  - There are MANY options to do it and it's good to have a high-level overview of all of them. Most important ones are: Binary Authorization, RBAC, Node auto-upgrade, Cloud NAT, Cloud Armor, VPC Service Controls, Workload Identity, GKE Sandbox etc)
- Know services supporting CMEK/CSEK (GCS & GCE/PDs).
- Know how to set up External Key Manager (where to create keys, UID, how to grant privileges to that key from GCS perspective). Link.
- How to manage secrets in Secret Manager according to best practices (separate Secret Manager project for prod and non-prod, granular per-secret IAM privs). Link.
- Know a bit about how to set up Managed Microsoft AD in GCP.
- No questions about Forseti (replaced by Cloud Inventory)
- Google Workspace-related questions, mostly about how to NOT allow users from external organizations to be added to groups in Cloud Identity, and how to reduce session length
- How to prevent external connections to publicly-exposed Cloud SQLs?
- How to set up a secure, low-cost solution to redirect **all** Internet-facing traffic through on-premises connection (Cloud VPN + routing through the VPN tunnel).

PCSE exam tips&tricks

- How to make sure all in-use data cannot be exfiltrated (Org Policy which requires Confidential Computing: constraints/compute.restrictNonConfidentialComputing)
- Steps to set up CMEK with EKM: link.
- How to make sure that ALL logs for a specific project stay in a chosen country (edit _Deafult sink to redirect it to a different, regional logging bucket)
- Detailed OS Image Family - related questions (concrete IAM roles, where to and whom to assign them to; how to use OS image from external org when VPC-SC are set up)
- Why / how to mute some findings (SOC2 vulnerabilities etc) in SCC.
- Questions about Web Security Scanner.

Google Cloud

NIST Cybersecurity Framework & Google Cloud

NIST Cybersecurity Framework & Google Cloud

Securing critical infrastructure and managing cybersecurity risks

Google Cloud

QUIZ week 6

(the one we went through during the meeting)

Reminder:

- NOT as complex as questions on the exam
- Technical knowledge validation (No business context)

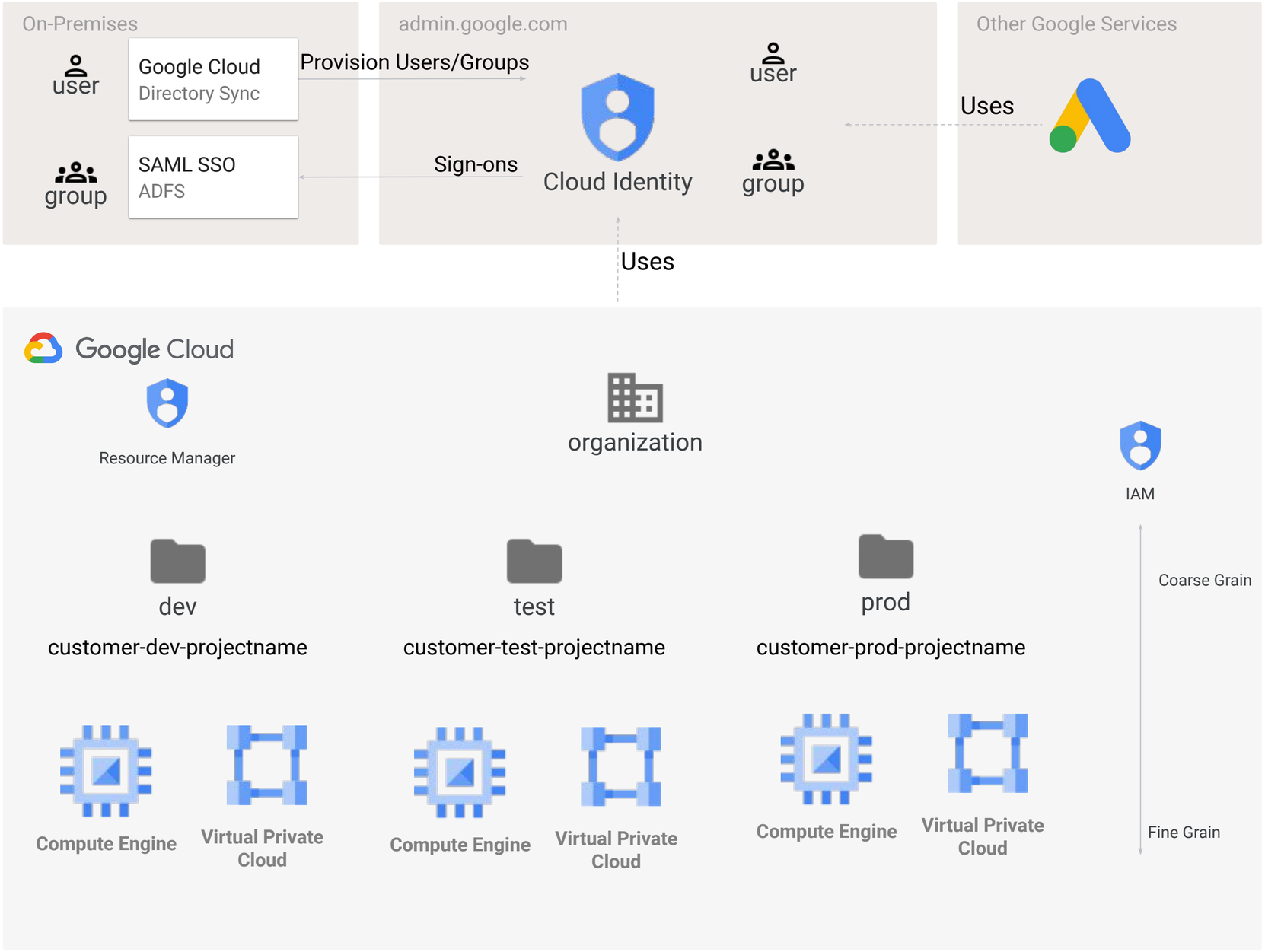
Bonus quiz

Pre-exam quiz

~30 exam-like questions which should help you evaluate your exam-readiness.

Study Cards

PCSE Study Cards - IAM & Cloud Identity



- SSO and GCDS are mutually exclusive (although often used together)
- Resource Manager is where your hierarchy is defined
  - An organization is technically optional
  - Folders are optional as well
    - Can be nested
- IAM Permissions can be assigned at any level (org, folder, project, resource)
  - Lower generally is least privilege
- Three types of roles: Basic (primitive), Pre-defined, Custom
  - Basic (owner, editor, viewer) are generally limited to non-production or special cases
  - Pre-defined are most common
  - Custom have some limitations (not all permissions, limited number)
- Best practices
  - Assign to groups rather than user accounts
  - Assign lowest level practical
  - Assign fewest permissions possible to “get the job done”
  - Assigning at a higher level effects all current and future resources

PCSE Study Cards - common BigQuery IAM roles

Role	Description
BigQuery Admin	Can do everything in BigQuery. Create and read data, run jobs, set IAM policies, etc.
BigQuery Data Owner	Read/write access to data, plus can grant access to other users and groups by setting IAM policies.
BigQuery Data Editor	Read/write access to data.
BigQuery Data Viewer	Read-only access to data.
BigQuery Job User	Can create and run jobs, but no access to data.
BigQuery User	Can run jobs, create datasets, list tables, save queries. But no default access to data.

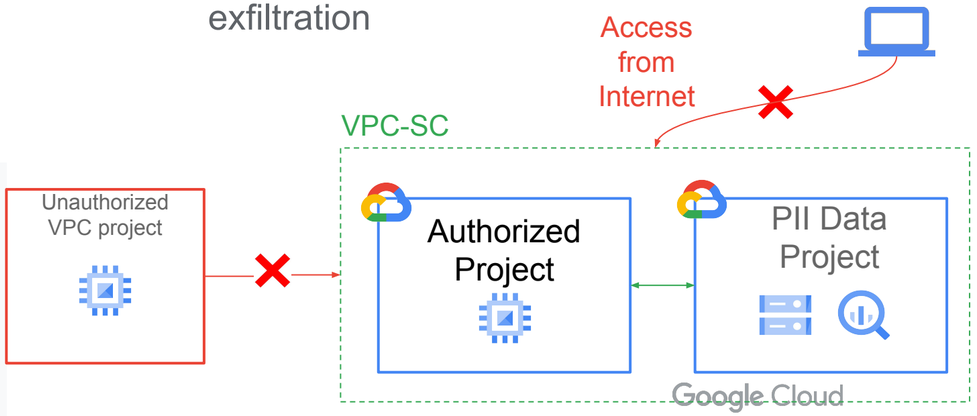
PCSE Study Cards - Securing Cloud Storage

Type	Scope	Access Control
IAM permission	Project, bucket	• Grant access to project's bucket and objects • ***User*** must be in IAM
Access control lists (object ACL)	Object	• Grant read or write access to users for objects • Can permit ***users*** from outside
Signed URLs	Object	• Grant time-limited read or write access to an object • ***Anyone*** you share URL with
Signed policy document	Bucket	• Policy control contents that can be uploaded

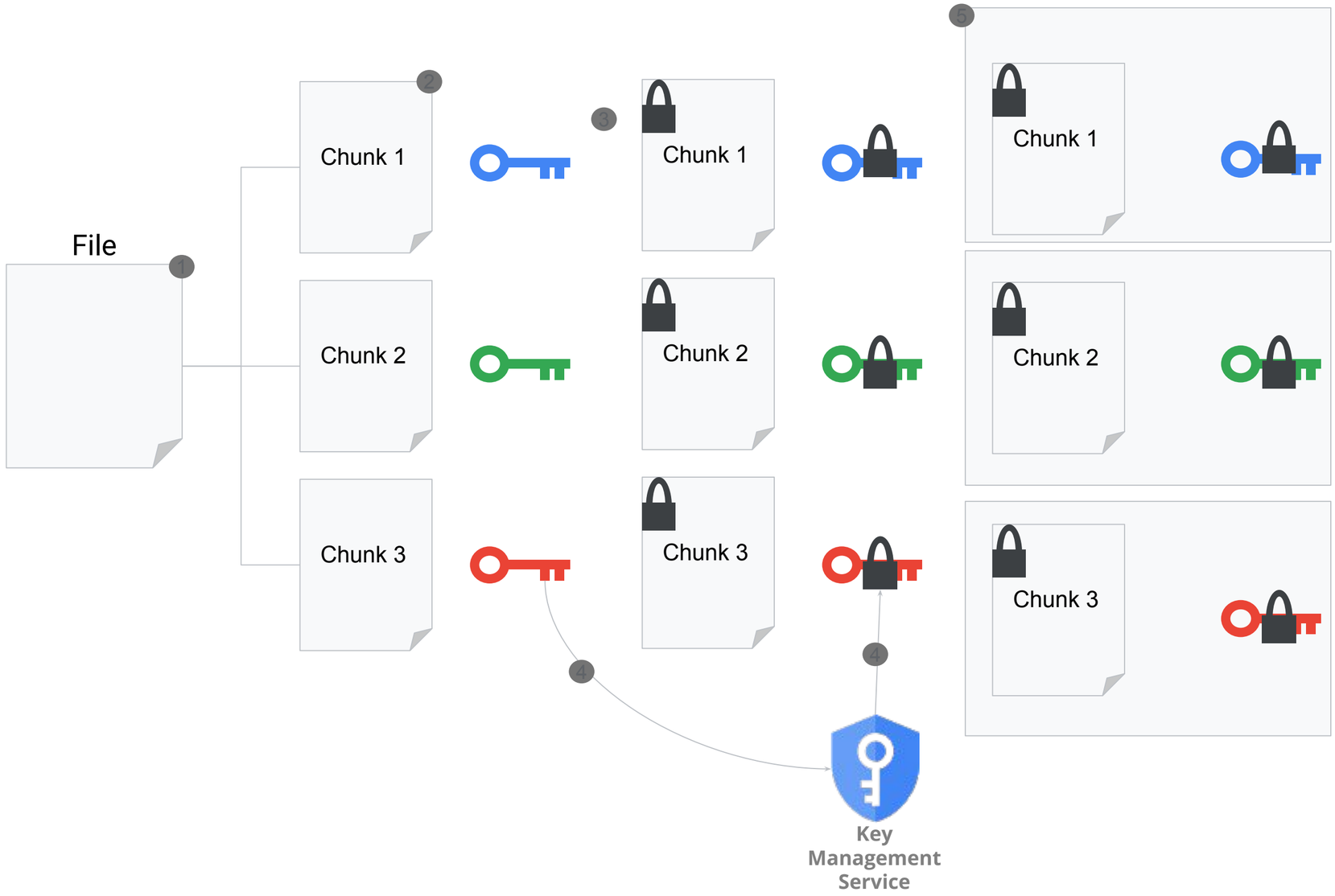
Cloud Storage Retention Lifecycle

Type	Does
Object Versioning	• Creates an archived version of an object each time the live version of the object is overwritten or deleted. • Uniquely identified by a generation number. • Retains its ACLs and does not necessarily have the same permissions as the live version of the object.
Lifecycle Management	• Controls when an object can be deleted. • Enforce data retention with a bucket lock. Locks are permanent! • Change the storage class of live and/or archived objects. This action can be applied to both versioned and non-versioned objects.

- ➔ Granting Access
  - ◆ IAM Permissions
  - ◆ ACLs
  - ◆ Signed URLs
  - ◆ Signed Policy Document
- ➔ Protecting from Ransomware
  - ◆ Retention Policies + Retention Policy Locks
  - ◆ Versioning
- ➔ Supported Encryption Options
  - ◆ Google Managed Encryption Key (GMEK) - **Default**
  - ◆ Customer Managed Encryption Key (CMEK)
  - ◆ Customer Supplied Encryption Key (CSEK)
  - ◆ Client side encryption (augments the above options)
- ➔ VPC-SC can be configured to prevent data exfiltration



PCSE Study Cards - Envelope Encryption



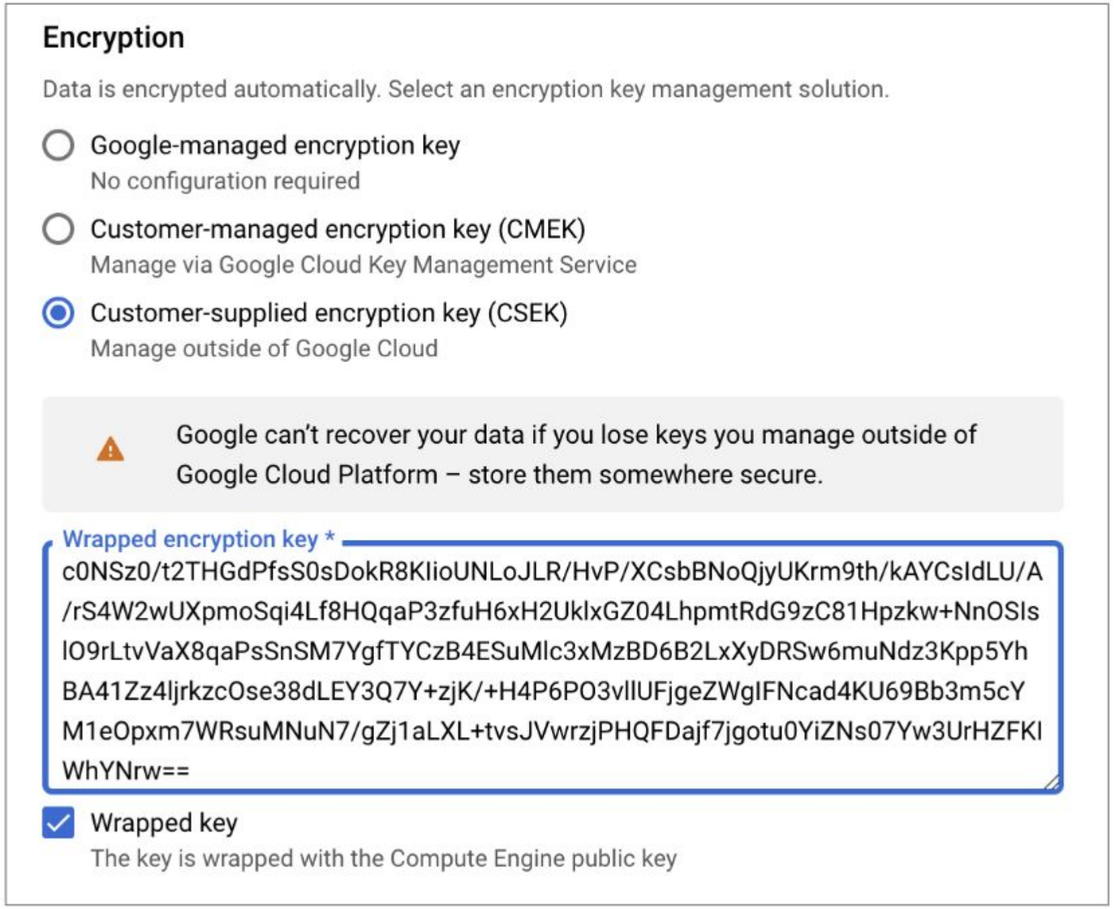
- File is uploaded (1)
- File is chunked (2)
- Each chunk is encrypted with a unique DEK (3)
- The DEK is then encrypted, also called “wrapped”, with the KEK (4)
- Wrapped DEK and the encrypted block are stored together (5)
- Multiple copies of each chunk /key are stored (not shown)
- The KEK ***never*** “leaves” KMS
- The encryption Algorithm used is AES256
- The process is the same for GMEK or CMEK
- For CSEK (GCS and GCE Only) the primary difference is the KEK is always supplied directly by the customer. Specified in the boto config file:

```
encryption key =
39So8jZi8tSi/vgr9F3bBsCJOV3I//UoqbtWGbWVvN0=
```

- When you use the CMEK you can specify:
  - Key rotation frequency (needed for certain regulations
  - Data Residency
  - Destroy keys (crypto deletes the data)

PCSE Study Cards - Using customer-supplied encryption keys

You must provide the key when creating or using the storage resource.



PCSE Study Cards - Creating a signed URL with “gcloud storage”

- Create a service account with rights to storage.
- Create a service account key.
- Use sign-url command, which returns a URL that allows access to the resource.
  - –duration parameter is used to specify how long the signed URL should be valid

```
gcloud iam service-accounts keys create ~/key.json --iam-account
storage-admin-sa@doug-demo-project.iam.gserviceaccount.com

gcloud storage sign-url gs://super-secure-bucket/noir.jpg
--private-key-file=~/key.json –duration=10m
```

PCSE Study Cards - GCS: Signed Policy Documents

- Signed Policy Documents specify what can be uploaded to a bucket with a form POST.
- Allow greater control over size, content type, and other upload characteristics than signed URLs.
- Created as JavaScript Object Notation (JSON).

```
{"expiration": "2023-08-15T11:11:11Z",
 "conditions": [
  ["starts-with", "$key", "" ],
  {"acl": "bucket-owner-read" },
  {"bucket": "travel-maps"},
  {"success_action_redirect": "http://www.example.com/success.html" },
  ["eq", "$Content-Type", "image/jpeg" ],
  ["content-length-range", 0, 1000000]
  ]
}
```

PCSE Study Cards - GCS: Using Policy Documents

01 Ensure the policy document is UTF-8 encoded.

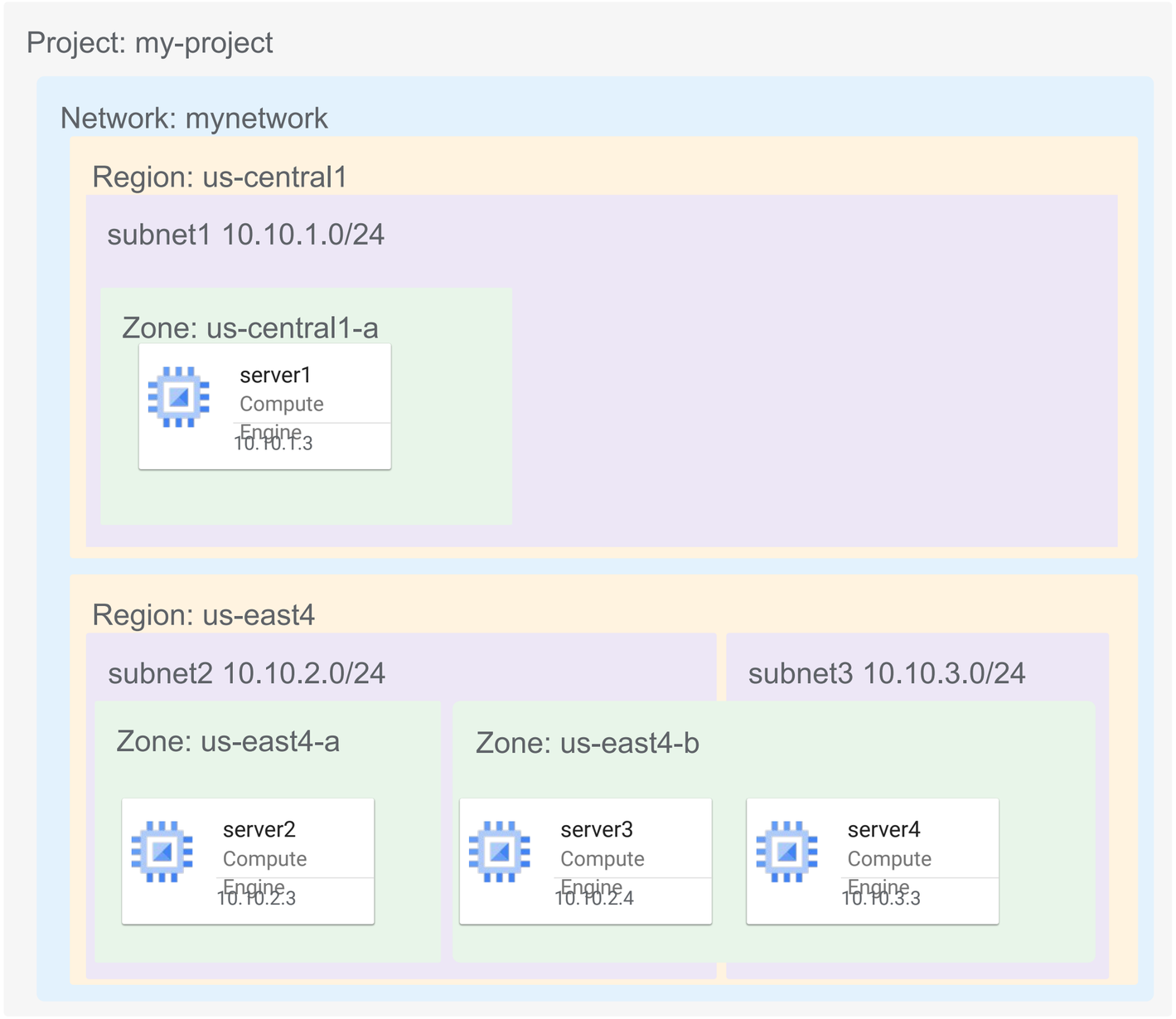
02 Encode the policy document as a Base64 representation.

03 Sign your policy document using RSA with SHA-256 using the secret key provided to you in the Google Cloud console.

04 Encode the message digest as a Base64 representation.

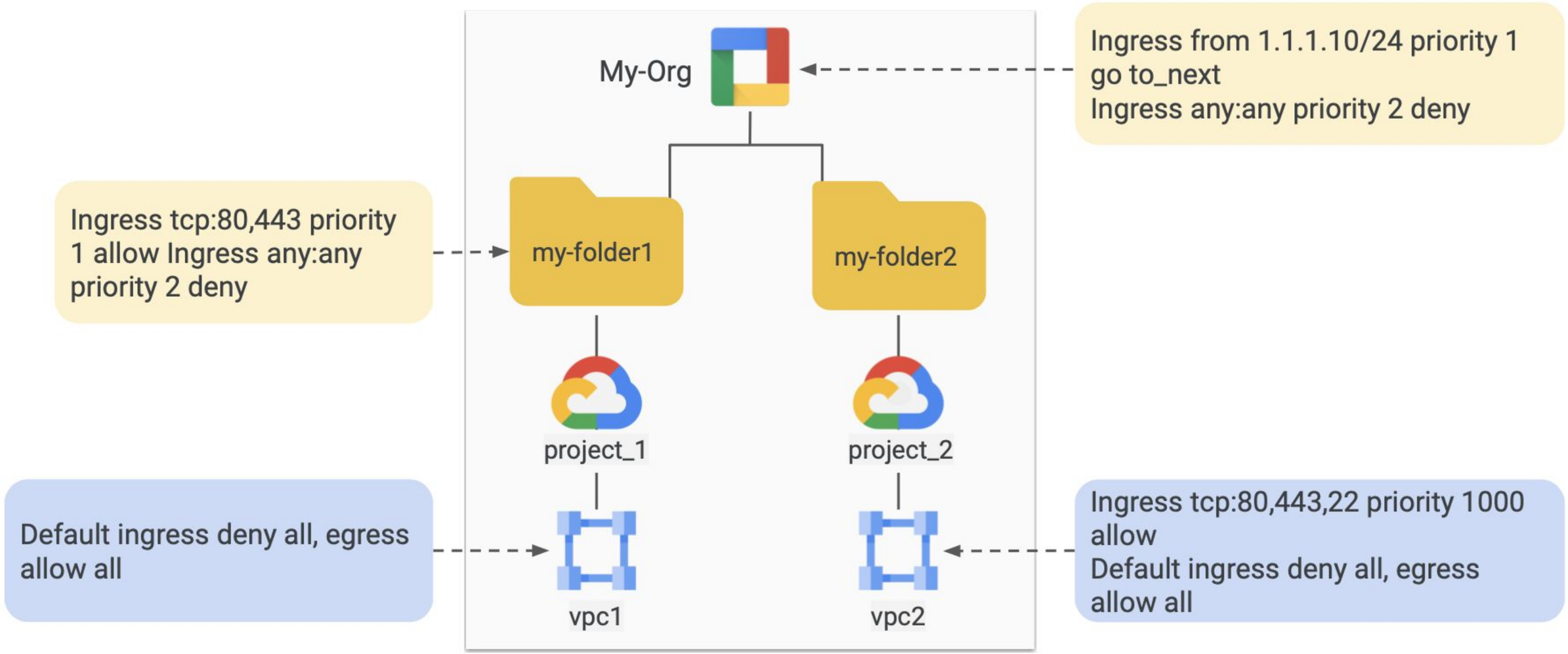
05 Add the policy document information to the HTML form.

PCSE Study Cards - networking basics

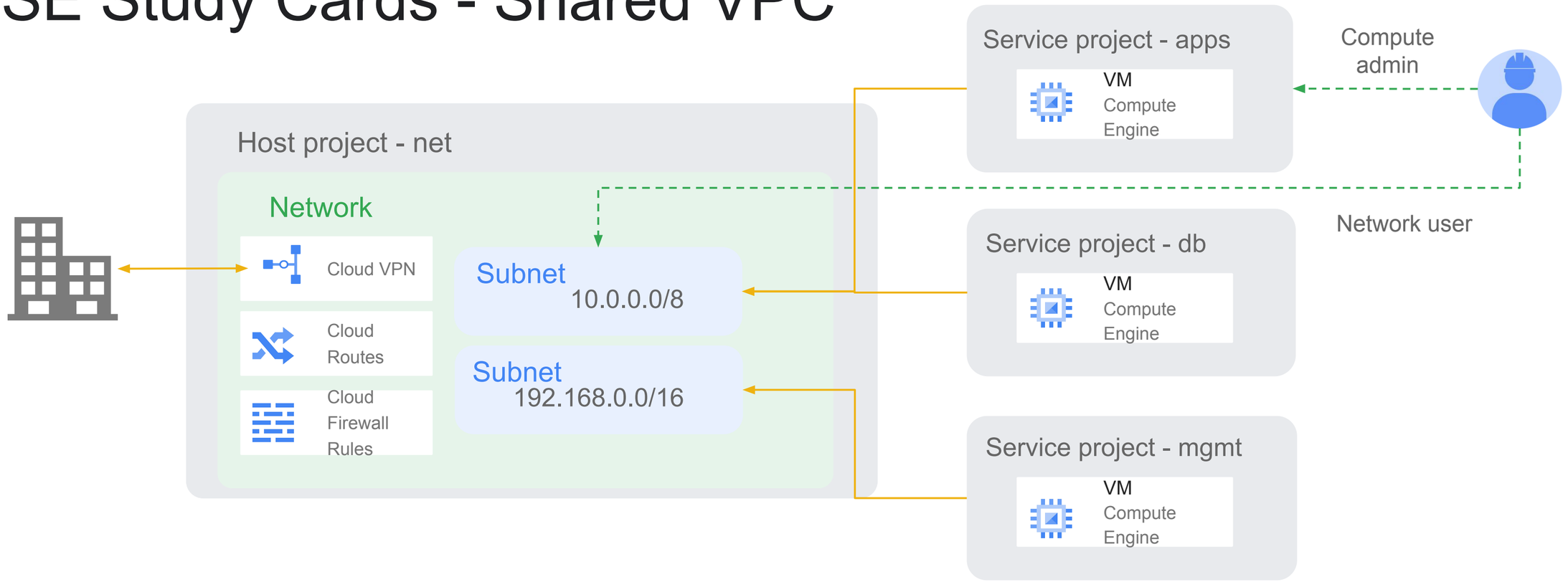


- A VPC belongs to 1 project
- A VPC can be present in every region across GCP (and is in the default configuration)
- No additional configuration is required for servers to communicate globally (VPNs or routers)
- A subnet crosses zones within a region, but cannot cross regional boundaries
- Implied Firewall Rules (65535):
  - Allow all egress traffic
  - Deny all ingress traffic
- Default rules
  - Allow SSH, ICMP, RDP
  - Block SMTP Traffic
- Lower the number of firewall rule the higher the priority (1 > 10)
- Components of a firewall rule:
  - Direction (ingress / egress)
  - Priority (0 to 65535)
  - Action (Allow / Deny)
  - Enforcement Status
  - Target
  - Source
  - Protocol
  - Log (1 or 0)

PCSE Study Cards: Hierarchical firewall policies

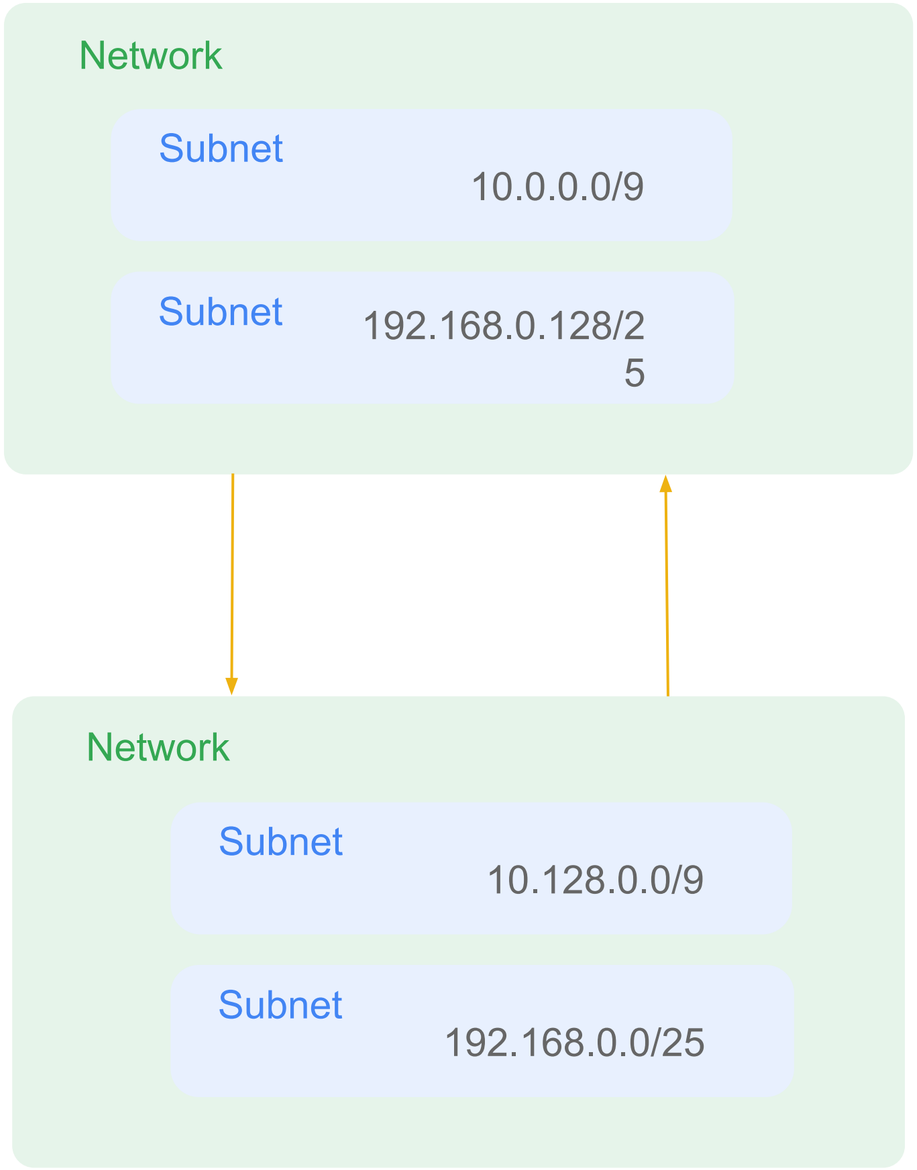


PCSE Study Cards - Shared VPC



- ➔ Shared VPC is the most common way to share networks. Allows you the flexibility of having many projects (good for security / billings / etc) without the overhead of managing a lot of VPCs.
- ➔ Allows you to setup a robust network in the host project and share subnet(s) with service projects.
- ➔ Allows good security segmentation as admins on compute nodes don't need to admin network functions (only need user permissions).
- ➔ Connectivity to other networks (VPN and interconnects) and firewall rules can be centrally managed in the host project.
- ➔ Host and service projects ***must*** belong to the same GCP organization

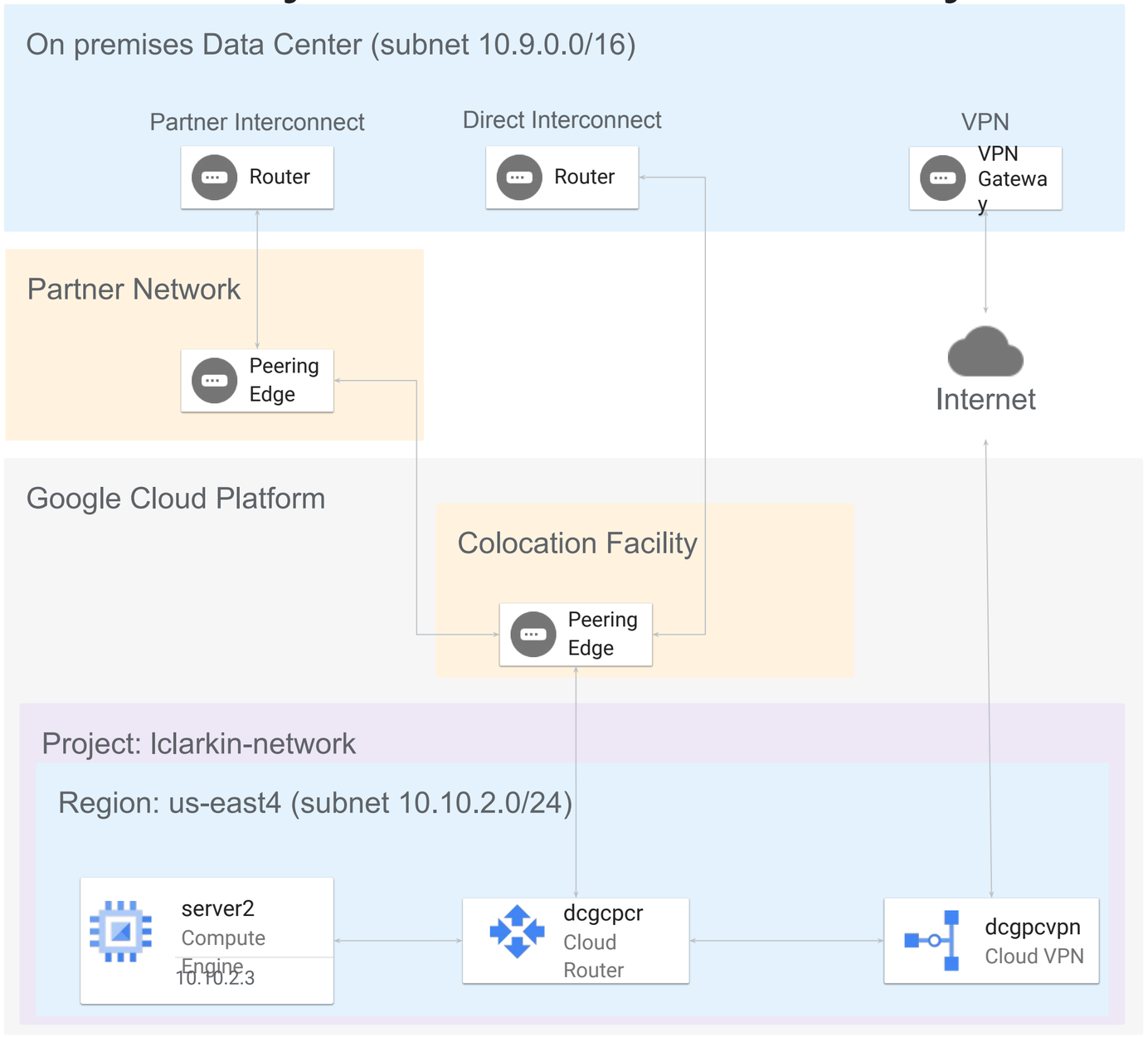
PCSE Study Cards - VPC Peering



- ➔ Peering works both within and between GCP organizations
- ➔ When setting up the peering you determine which subnet(s) to publish routes to
- ➔ Administrators on both sides must configure the peering in order for it to work
- ➔ The peering between the networks is **not** transitive, so traffic will not route to any other networks peered
- ➔ Links between the networks are high throughput and very low latency (unlike connecting via a VPN)
- ➔ IP Networks ***cannot*** overlap

Note: Starting to see peering as part of the solution for GCP Products: Apigee X and Datastream configurations both require peering as part of the setup

PCSE Study Cards - Connectivity

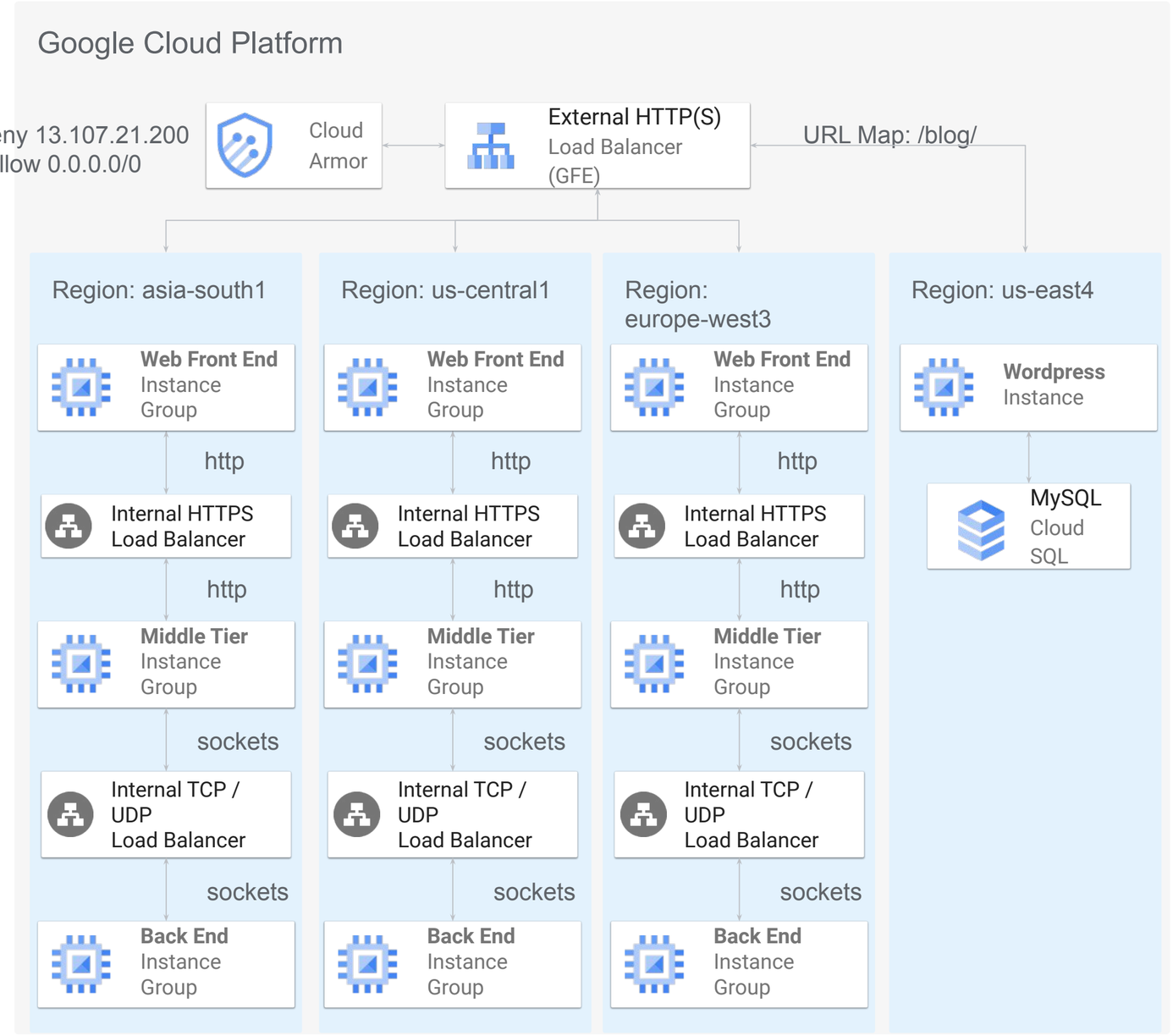


- Speeds (*)
  - VPN up to 3 gbps
  - Partner up to 50 gbps
  - Dedicated up to 100 gbps
- VPN Connections always go over the internet
  - The connection is encrypted using IPSec
  - There are pre-shared keys exchanged to facilitate
  - Must have a public IP address
- Interconnects (both direct and partner) are always to GCP, not Google
  - Consumer services / Workspace still go over the internet
- You should ***never*** have only 1 connection into GCP
  - Connections should be in two separate regions (not zones)
  - You can use a different solution to backup the primary (primary interconnect, vpn as backup)
- IP Address ranges cannot overlap in any of the architectures

* Can stack some of these solution for higher speeds

Google Cloud

PCSE Study Cards - Load Balancing



- External HTTP(S) Load Balancer
  - Global Service (*)
  - Traffic to “closest” endpoint
  - Single Anycast IP Address
  - Can be used for workloads on-premises or other clouds
- URL Map apply to both Internal and External HTTP(s) Load balancers
  - Directs to different backends
  - Based on a fragment of the url or host names
- Cloud Armor
  - rules to protect vulnerable backend services from OWASP Top 10 attacks like SQL Injection and cross site scripting
  - Allow / Deny lists for IP addresses and regions
  - Like Firewall rules, lower the number higher the priority (1>10)
  - Named IP list are 3rd party maintained list for malicious IP addresses
- Additional items to remember:
  - Health Checks on backends
  - Firewall rules
  - SSL Proxy (not shown) is for non-http traffic

* requires premium network tier

Google Cloud

PCSE Study Cards: Pre-configured managed SSL profiles

COMPATIBLE

Allows the broadest set of clients.

MODERN

Supports a wide set of SSL/TLS features, allowing modern clients to negotiate SSL/TLS.

RESTRICTED

Supports a reduced set of SSL/TLS features, intended to meet stricter compliance requirements.

- If no SSL policy at all is set, a default SSL profile is applied that is equivalent to an SSL policy that is using the COMPATIBLE profile.
- Custom SSL policy profiles can also be created. They let you select the exact set of SSL features you would like to support.

PCSE Study Cards - Cloud DLP

De-Identification Techniques

Transformation	Original Value	New Value	Notes
Text Redaction	(262) 555-1212		Removes the text
Basic Replacement	(262) 555-1212	(999) 999-9999	Replaces with the same text for all
Infotype Replacement	(262) 555-1212	PHONE_NUMBER	Preserves Type
Masking	(262) 555-1212	(262) ***-****	Substitutes some or all characters
Generalization	92	High	Keeps relative value without revealing the exact value
Pseudonymization	(262) 555-1212	NAM_PHONE_NUMB(14):+*pb[NZdc95tLB	Replaces sensitive values with cryptographic tokens
Date Shifting	07/04/1992	09/23/1992	Keeps relative value without revealing the exact value

- Cloud DLP Contains over 150 built in InfoTypes
  - Global Identifier
  - Country Specific
- Cloud DLP can be used to only identify sensitive data (does not need to transform) and identification is **always** the first step
- The Match likelihood is computed
  - VERY_UNLIKELY
  - UNLIKELY
  - POSSIBLE
  - LIKELY
  - VERY_LIKELY
- Pseudonymization:
  - Can preserve referential integrity as the value will be deterministic
  - Can be “one way” so that the data is not recoverable.
  - Can be reversible if your use case requires it
  - Can preserve the format of the value
- Not Shown: image redactions
  - Finds and blocks out sensitive data inside pictures

Most common Organization Policy constraints

Policy Constraint	Description
compute.vmExternalIpAccess	A list of project/zone/instance names that are allowed to have external IP addresses and deny all others. Attempts to create any other VMs with an external IP address will fail.
compute.trustedImageProjects	A list of projects that contain trusted images that can be used as the basis for a VM and deny all others. Attempting to instantiate a VM with an image from another project is denied.
compute.skipDefaultNetworkCreation	Disables the creation of default VPC when creating a project. The default VPC uses auto mode subnetworks and includes default firewall rules which are often incompatible with production deployments.
iam.disableServiceAccountKeyCreation	This boolean constraint disables the creation of service account external keys where this constraint is set to `True`.
compute.restrictVpcPeering	This list constraint defines the set of VPC networks that are allowed to be peered with the VPC networks belonging to this project, folder, or organization.
serviceuser.services	This list constraint defines the set of services and their APIs that can be enabled on this resource and below. By default, all services are allowed.
gcp.resourceLocations	BETA: This list constraint defines the set of locations where location-based GCP resources can be created. Policies for this constraint can specify multi-regions such as asia and europe, regions such as us-east1 or europe-west1, or individual zones such as europe-west1-b as allowed or denied locations.
sql.restrictPublicIp	This boolean constraint restricts configuring Public IP on Cloud SQL instances where this constraint is set to True. This constraint is not retroactive, Cloud SQL instances with existing Public IP access will still work even after this constraint is enforced. By default, Public IP access is allowed to Cloud SQL instances.
sql.disableDefaultEncryptionCreation	BETA: Restrict default Google-managed encryption on Cloud SQL instances
compute.requireShieldedVm	This boolean constraint, when set to True, requires that all new Compute Engine VM instances use Shielded disk images with Secure Boot, vTPM, and Integrity Monitoring options enabled. Secure Boot can be disabled after creation, if desired. Shielded VM features add verifiable integrity and exfiltration resistance to your VMs.
compute.restrictSharedVpcHostProjects	Restrict Shared VPC Host Projects This list constraint defines the set of Shared VPC host projects that projects at or below this resource can attach to. By default, a project can attach to any host project in the same organization, thereby becoming a service project.
iam.allowedPolicyMemberDomains	This list constraint defines the set of members that can be added to Cloud IAM policies. By default, all user identities are allowed to be added to Cloud IAM policies. The allowed/denied list must specify one or more Cloud Identity or G Suite customer IDs. If this constraint is active, only identities in the allowed list will be eligible to be added to Cloud IAM policies.

Additional content 1

[READING]

- Shift security left! https://cloud.google.com/blog/products/identity-security/scan-for-vulnerabilities-early-to-shift-security-left-in-cicd
- Forensics in GCP howto: https://cloud.google.com/blog/products/identity-security/how-to-use-live-forensics-to-analyze-a-cyberattack
- Cloud Logging - exporting logs
- Building internet connectivity for private VMs
- [Recommended] Logs data: A step by step guide for overcoming common compliance challenges

[VIDEOS]

- Cloud IDS (relatively new product, most probably not yet covered by the exam): Getting started with Cloud IDS
- A concept of Workload Identity and how it's used to enhance security of GKE: Secure access to GKE workloads with Workload Identity
- (deep dive with a great demo; lenghty: 50mins, but it's worth it even if you watch only first ~20 mins) Improve Security Posture in GKE Environment with ACM and ASM
- Google Cloud Security Professional Certification - whole playlist related to PCSE exam; some may be outdated
- Google Cloud Security Showcase - another playlist with lots of short, useful videos for PCSE

Additional content 2

- Security and Trust on Google Cloud (Cloud Next ‘19 UK) - a mix of different services compiled into a nice story
- OAuth, JWT, HMAC, oh my! API security for your enterprise
- How to use Certificate Authority Service to create private certificates

[DEEP DIVES]

- Multi-step data deletion on Google Cloud (a good practice that may be handy).
- Anthos-related security mechanisms.
- [free: PDF, MOBI, EPUB] SRE book: Building Secure and Reliable Systems - feel free to pick and choose chapters of your interest. The ones specifically related to security are:
  - Chapter 1: The Intersection of Security and Reliability
  - Chapter 2: Understanding Adversaries
  - Chapter 5: Design for Least Privilege
  - Chapter 7: Designing for a Changing Landscape
  - Chapter 10: Mitigating Denial-of-Service Attacks
  - Chapter 11: Case Study: Designing, Implementing, and Maintaining a Publicly Trusted CA
  - Chapter 15: Investigating Systems (mainly: from page 471, "Collect Appropriate and Useful Logs")
  - Chapter 20: Understanding Roles and Responsibilities
  - Chapter 21: Building a Culture of Security and Reliability

Feedback

We value your feedback on this course and ask that you take a few minutes to fill out the survey for this course. You will find the link in your classroom, and can ask your instructor if you have any questions.

Q & A

Make sure to…

Enjoy the journey as much as the destination!