

Official Google Cloud Certified Professional Cloud Security Engineer Exam Guide

Chapter 1: About the GCP Professional Cloud Security Engineer Exam

[Home](#) | [OLP Resources](#) | [Help](#) | [Create New Account](#)



Powered By **KRYTERION™**
GLOBAL TESTING SOLUTIONS

Ready to start?

Please log in with your Google Cloud Webassessor account to see our catalog and register for an exam.

[Forgot password?](#)

LOGIN

Make sure you review the [retake policy](#) and [recertification eligibility criteria](#) before you take an exam. There is a limit on the number of times you can take the exam and a waiting period between attempts (even if you are taking the same exam in a different language). It is the user's responsibility to adhere to these [terms and conditions](#) to avoid possible suspension or rejection of exam results.

Don't have an account?

Click [here](#) to create a Google Cloud Webassessor account for exams in English.

To see what other languages are available, go [here](#).

Figure 1.1 – Logging in to Webassessor



Powered By **KRYTERION™**
GLOBAL TESTING SOLUTIONS

Receipts Register For An Exam My Assessments Home

You last logged in 24 September 2021 at 10:40PM MST.

Make sure you review the [retake policy](#) and [recertification eligibility criteria](#) before you take an exam. There is a limit on the number of times you can take an exam and a waiting period between attempts (even if you are taking the same exam in a different language). It is your responsibility to adhere to these [terms and conditions](#) to avoid possible suspension or rejection of exam results.

Launching your online exam? Due to high volume, you may experience additional wait time (15-20 mins) before connecting with a proctor. Do not disconnect. We appreciate your patience!

REGISTER FOR AN EXAM

Kryterion, Inc. uses cookies to track session reliability, maintain session security, and understand user interaction with our website. By browsing our website, you consent to our use of cookies and other tracking technologies. For more information please see our [Privacy Policy](#).

[Privacy Policy](#) | [Terms of Service](#) © 2021 KRYTERION, Inc. and KRYTERION, Limited - All Rights Reserved.

Figure 1.2 – Registration page

- Google Cloud Certified - Professional Cloud Security Engineer (English)	This is the Google Cloud Certified - Professional Cloud Security Engineer exam. Please refer to the exam guide for current topics that may appear on the exam. You may attempt an exam at a test center or online and each attempt regardless of delivery method or language counts toward the total permissible attempts and the waiting period between attempts still applies (see our Retake Policy here).	<i>multiple</i>
Google Cloud Certified - Professional Cloud Security Engineer (English)	Pre-requisites: Retake Policy:	Onsite Proctored USD 200.00 Buy Now
Google Cloud Certified - Professional Cloud Security Engineer (English)	Pre-requisites: Retake Policy:	Remote Proctored USD 200.00 Buy Now

Figure 1.3 – Exam selection

Choose options below to narrow down the list of testing centers displayed.

Country: Province/State: City: OR

Postal Code Range

Select the Testing Center where you wish to take the test.

AVAILABLE TESTING CENTERS

<input type="checkbox"/>	Testing Location Name	Address	City	Province/State	Country	Map	Important Location Information
<input type="checkbox"/>	Alliance Computing Solutions_New York City	545 8th Avenue, #1210	New York	New York	United States	Map	

Figure 1.4 – Select a testing center

Selected Testing Center

Trainocate_Singapore
190 Middle Road,
#20-02 Fortune
Centre
Singapore, N/A
188979

Select Date

October, 2021

wk	Sun	Mon	Tue	Wed	Thu	Fri	Sat
38						1	2
39	3	4	5	6	7	8	9
40	10	11	12	13	14	15	16
41	17	18	19	20	21	22	23
42	24	25	26	27	28	29	30
43	31						

Select date

Select Start Time

12:00 PM
12:15 PM
12:30 PM
12:45 PM

Figure 1.5 – Book a date and time for the exam

Exam	Details	Price	Actions
Exam: Google Cloud Certified - Professional Cloud Security Engineer (English) Length : 120 minutes	Schedule : Friday, 25 August 2023 Start Time : 11:00 (UTC+08:00) Location : [Change] IVT Pte Ltd center -- Singapore 28A KHANDAHAR STREET SINGAPORE , N/A 198889	200.00	Remove

If you are not using a voucher/coupon, please skip and select "Check Out" to proceed.

Coupon/Voucher Code: [Apply](#)

Subtotal: 200.00
Estimated Tax: 0.00

Total Price: USD 200.00

*Charges are made in USD, currency conversion fees may apply

[Empty Cart](#) [Add Another Exam](#) [Return Home](#) [Check Out](#)

Figure 1.6 – Review and pay

Chapter 2: Google Cloud Security Concepts



Figure 2.1 – End-to-end provenance and attestation



Figure 2.2 – Google Cloud's shared security responsibility (IaaS)

Defense in depth at scale

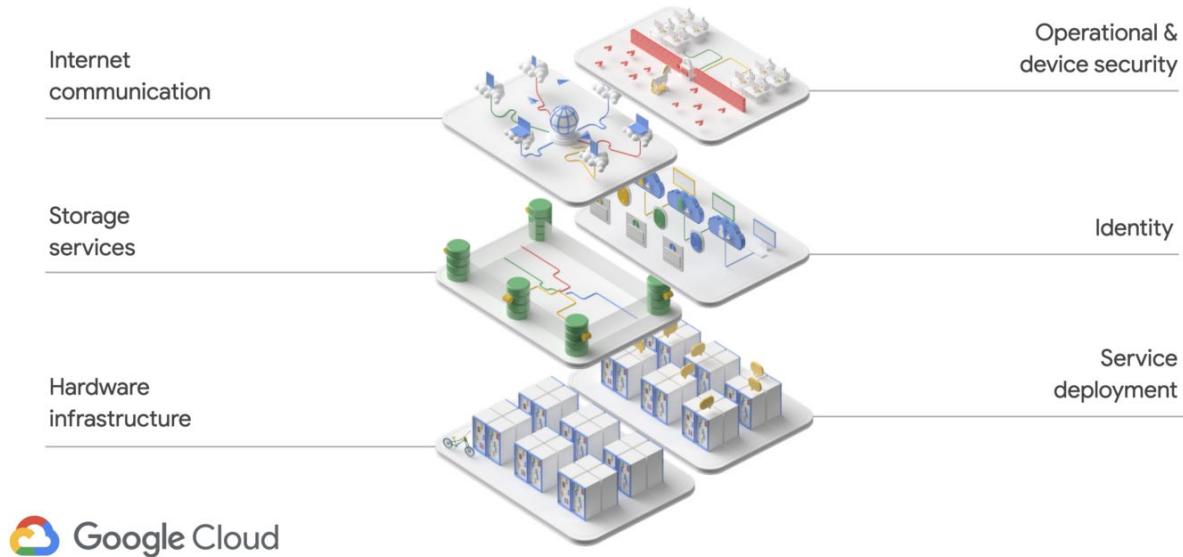


Figure 2.3 – Google defense in depth

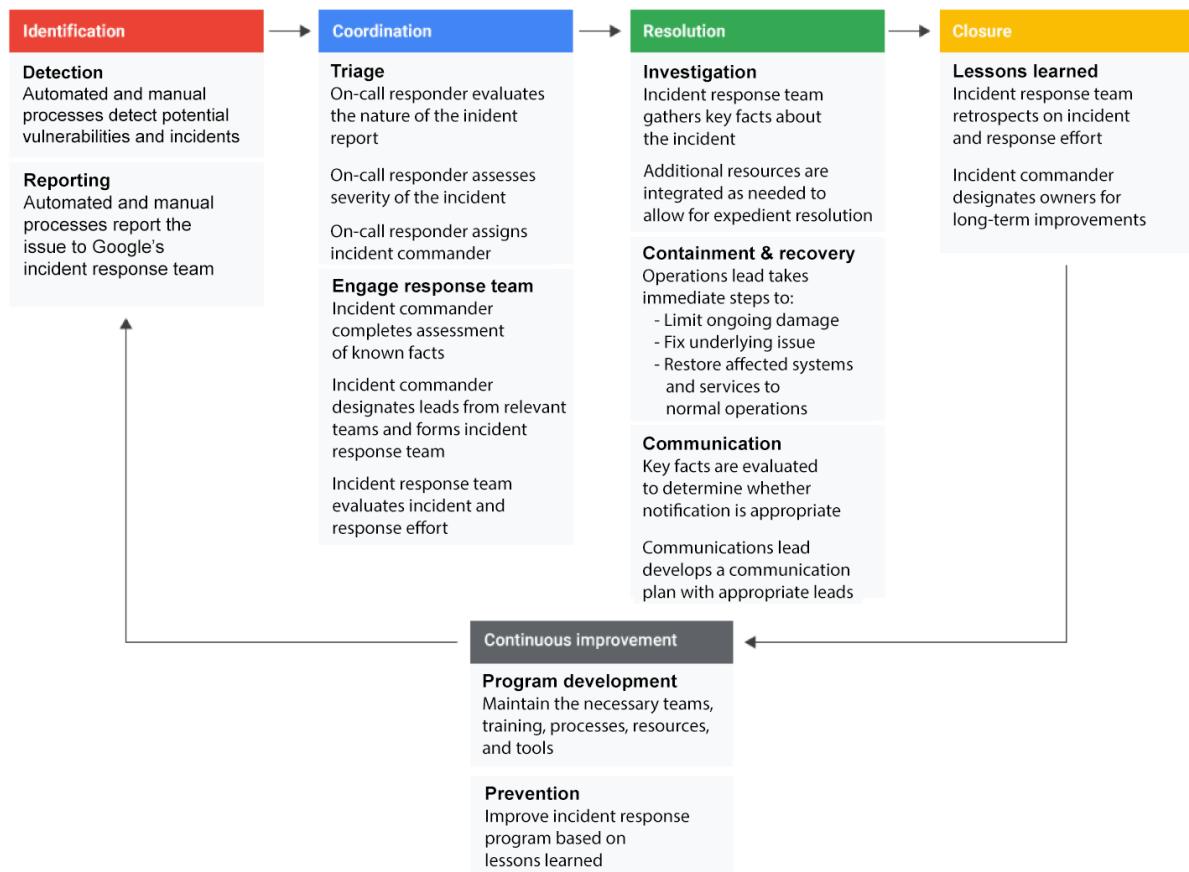


Figure 2.4 – Google Incident response workflow

Chapter 3: Trust and Compliance

Access Transparency

[Access Transparency](#) can be enabled for your Organization.

ENABLE ACCESS TRANSPARENCY FOR ORGANIZATION

Figure 3.1 – Access Transparency enabled confirmation

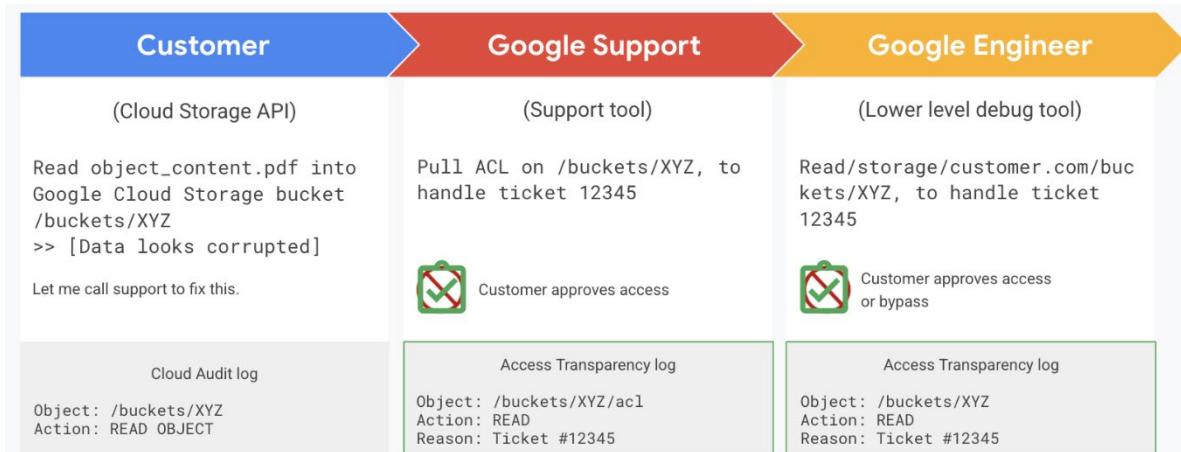


Figure 3.2 – Access Approval workflow

Security

Access Approval

Access Approval is a product that allows you to require your explicit approval whenever Google support and engineering need to access your customer data (some exceptions apply). This product is available to customers with qualifying support plans. [Learn more ↗](#)

[ENROLL](#)

[CONTACT SUPPORT](#)

Figure 3.3 – Access Approval enrollment

Enroll in Access Approval

By enabling this feature, support response times may increase because Google support will wait for your approval to access your customer data. [Learn more](#)



Figure 3.4 – Access Approval enrollment success

Key ring name *

Key ring location * ▾

Figure 3.5 – Google Cloud KMS geo-location configuration for key ring

						
Global	USA	Canada	Europe	Spain	Australia	Japan
ISO 27001	HIPAA	Personal Information & Electronic Documents Act	GDPR EU Model Contract Clauses Privacy Shield	Esquema Nacional de Seguridad	Australian Privacy Principles	FISC
ISO 27017	HiTrust		TISAX		Australian Prudential Regulatory Authority Standards	My Number Act
ISO 27018	FedRAMP				IRAP	
SOC 1	FIPS 140-2					
SOC 2	COPPA					
SOC 3	FERPA					
PCI DSS	NIST 800-53	Argentina	Germany	UK		
CSA STAR	NIST 800-171	Personal Data Protection Law	BSI C5	NCSC Cloud Security Principles		
MPAA	Sarbanes-Oxley					
GxP	SEC Rule 17a-4(f)					
Independent Security Evaluators	CFTC Rule 1.31(c)-(d)					
Audit	FINRA Rule 4511(c)					
Americas		Europe, Middle East & Africa			Asia Pacific	



Figure 3.6 – Third-party certifications and regulatory compliance

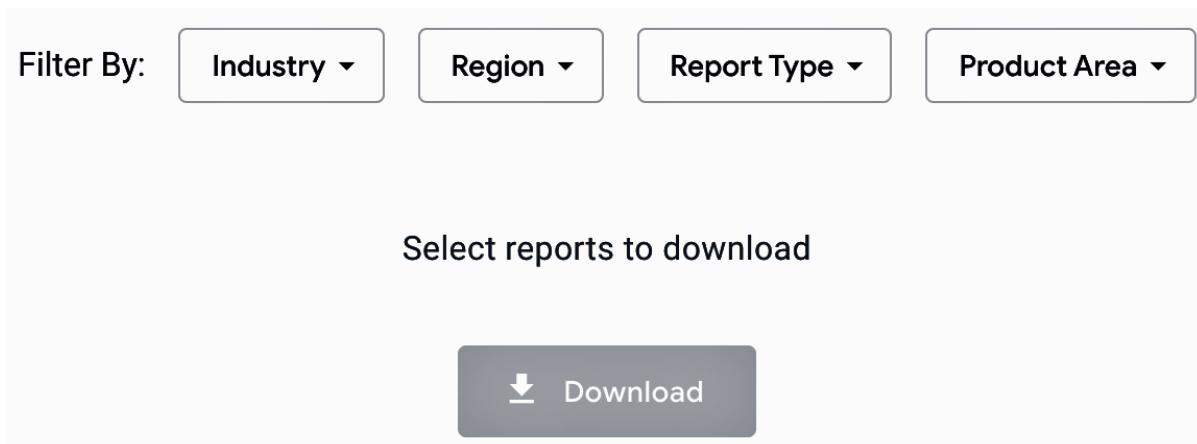


Figure 3.7 – Compliance Reports Manager

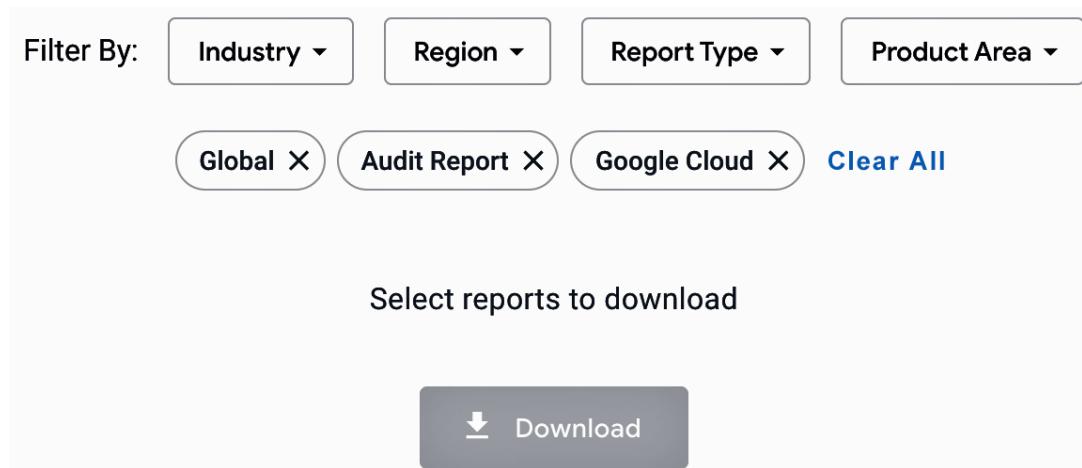


Figure 3.8 – Google Cloud Compliance Report Manager filter

Search for compliance reports in the table		<input type="checkbox"/> Downloadable reports only	
Compliance	Report type	Product area	Last audit
<input checked="" type="checkbox"/> PCI-DSS v3.2 PCI DSS is a set of network security and business best practices guidelines adopted by the PCI Security Standards Council to establish a "minimum security standard" to protect customers' payment card information. The Attestation of Compliance provides formal assurance from a Qualified Security Assessor (QSA) as to adherence to the PCI DSS.	Audit Report	Google Cloud	2 May 2021

Figure 3.9 – Compliance manager: PCI-DSS report download

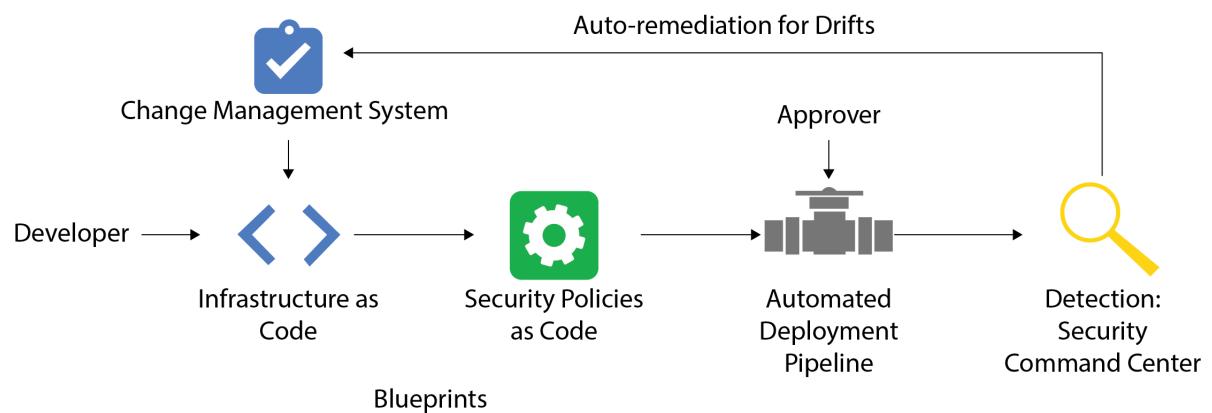


Figure 3.10 – Continuous compliance pipeline

Chapter 4: Resource Management

Organization hierarchy

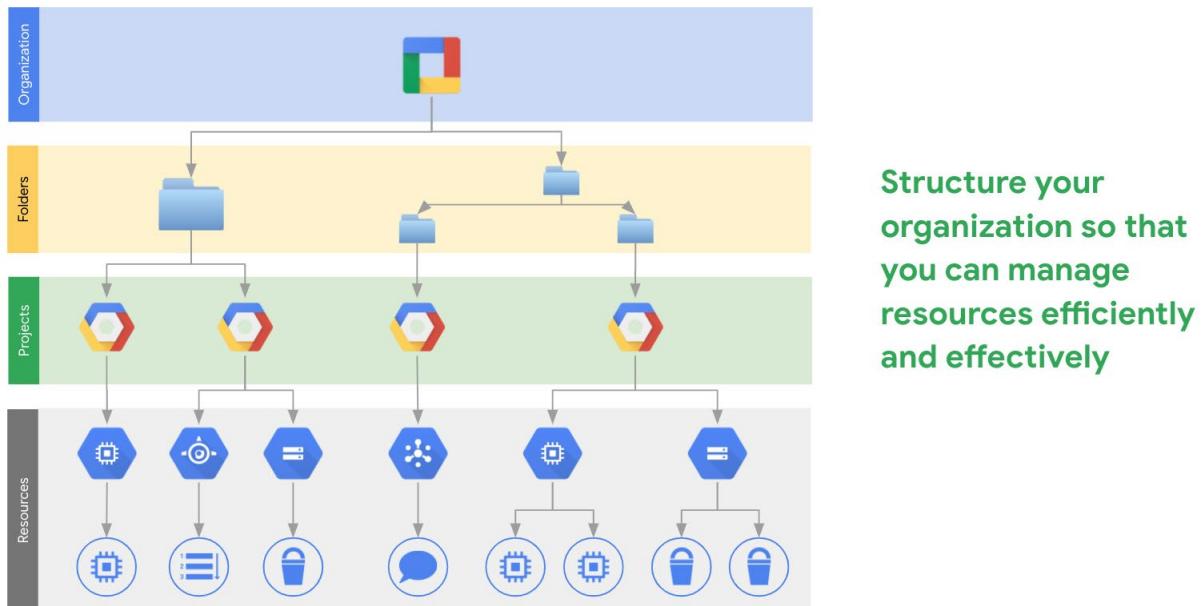


Figure 4.1 – Organization hierarchy

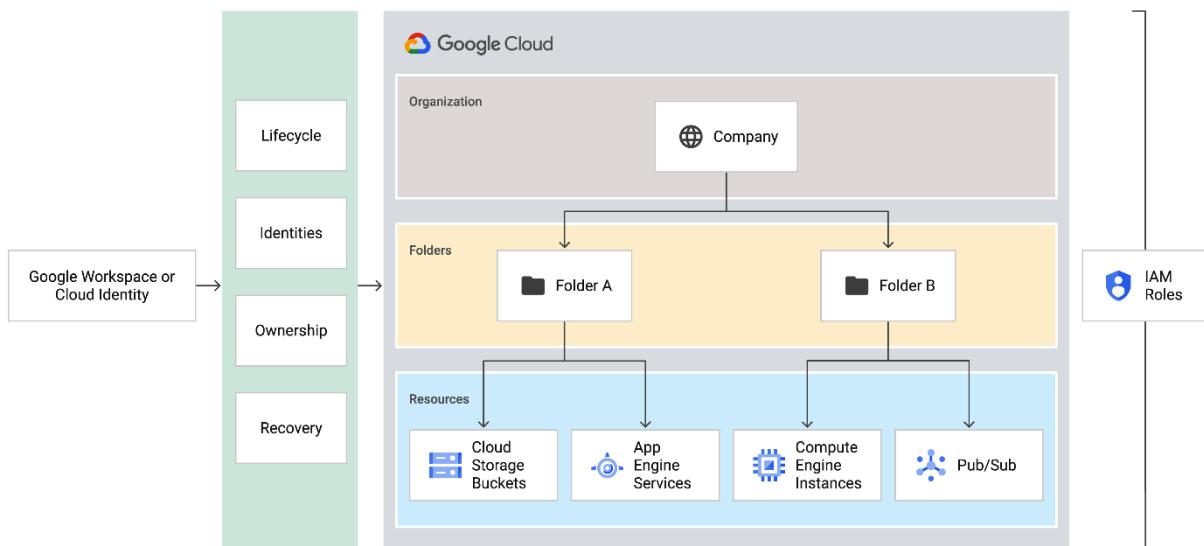


Figure 4.2 – Organizations

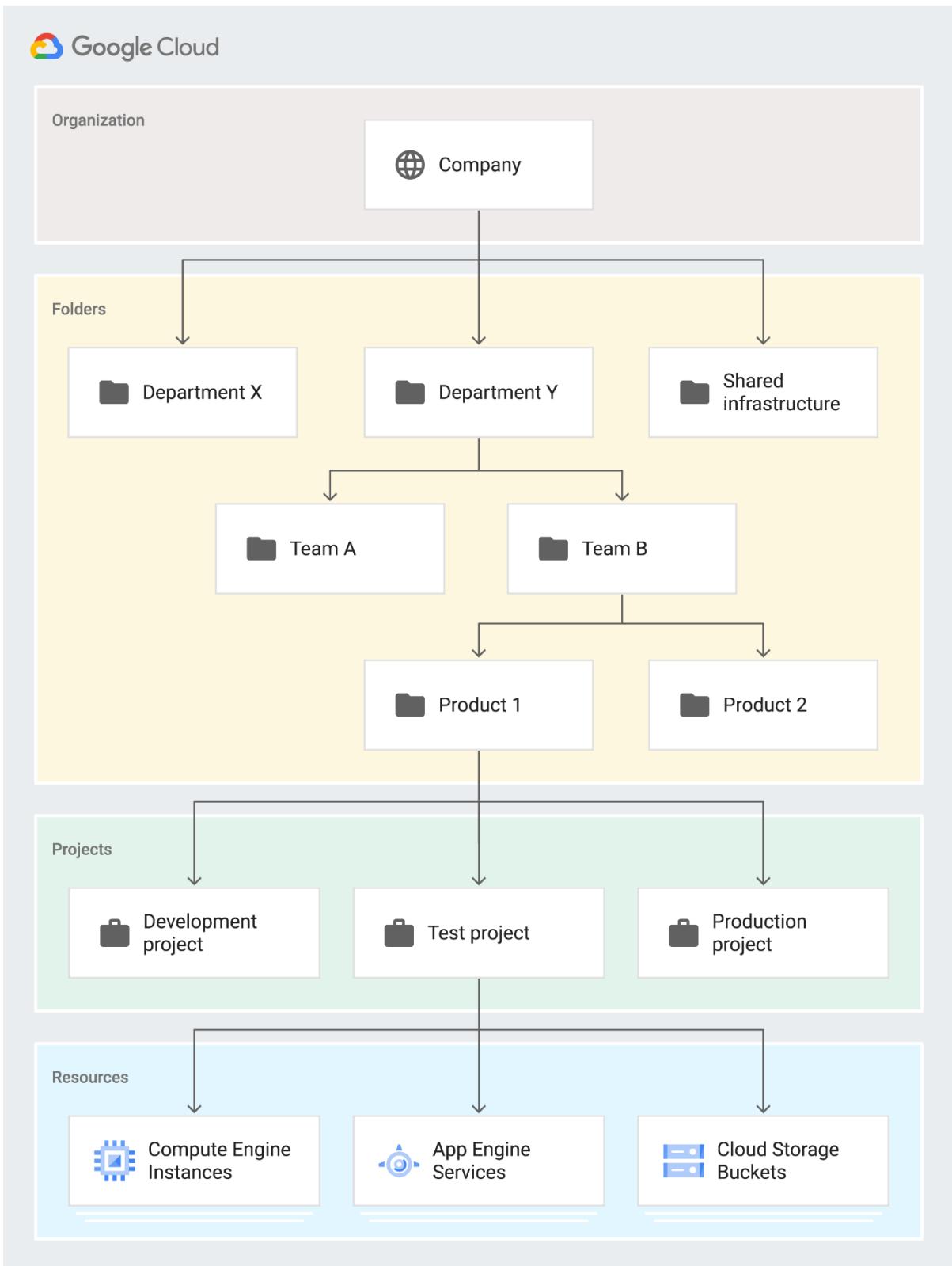


Figure 4.3 – Example enterprise organization

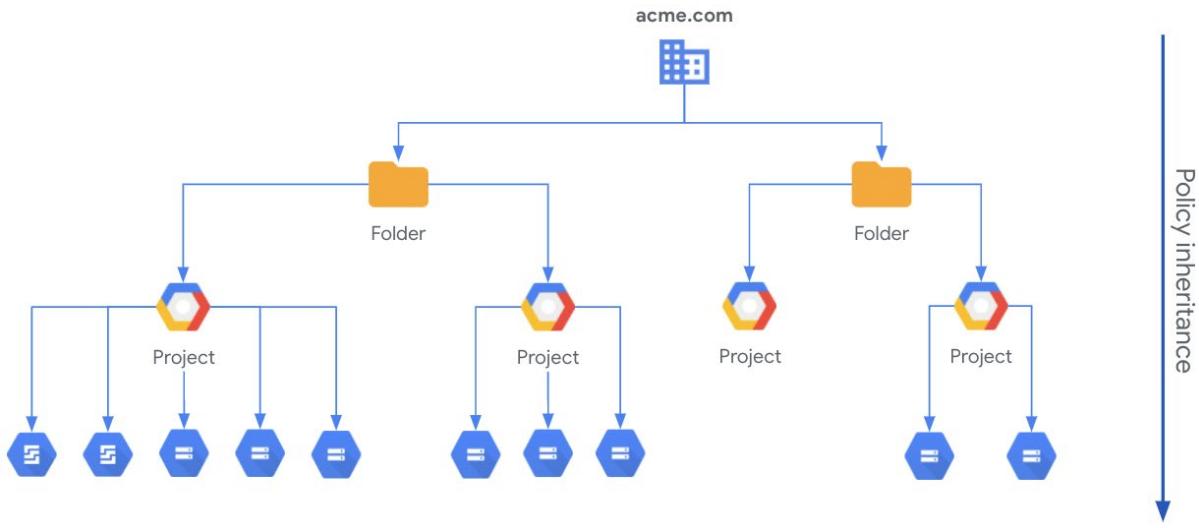


Figure 4.4 – IAM policy inheritance

Policy inheritance: Compute Engine example

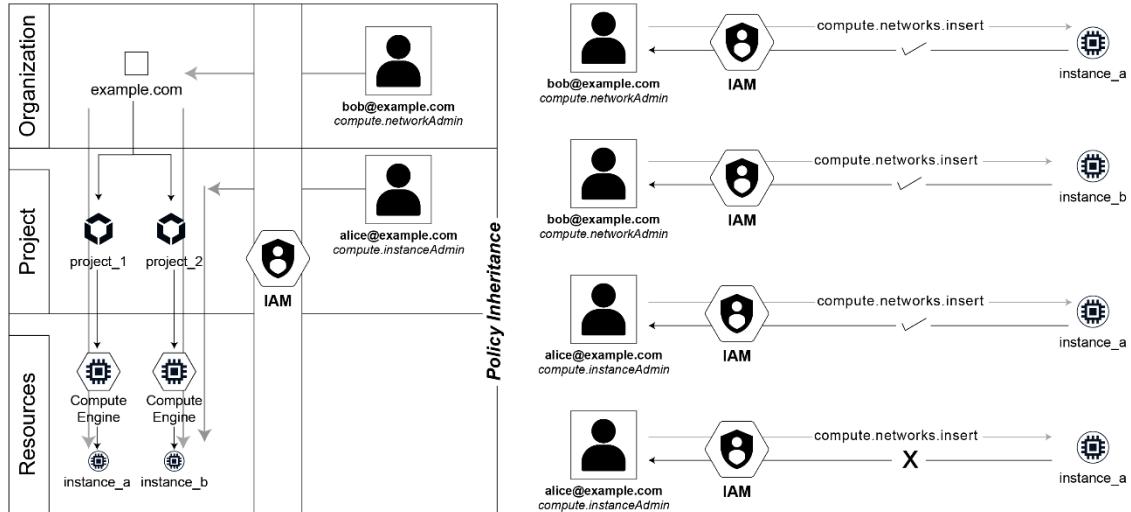


Figure 4.5 – IAM policy inheritance—Compute Engine

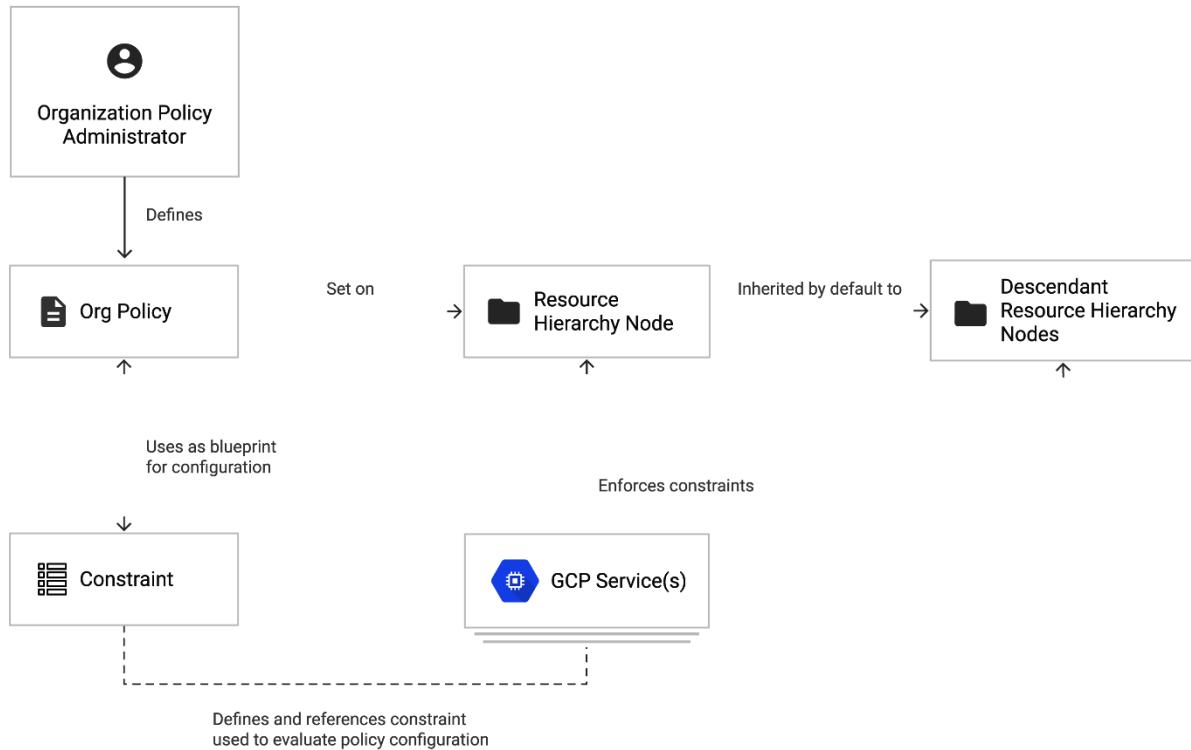


Figure 4.6 – Organization policy

Services	Constraints	Description	Useful for
Google Compute Engine	External IPs for VM instances	Defines a set of VM instances allowed to use external IP addresses.	Ensuring minimal external surface . VMs should normally get internal IPs only.
	Skip default network creation	Skips the creation of the default network and related resources during project creation.	Enforcing usage of centrally managed and secured VPC networks .
	Require OS Login	Enables OS Login on all newly created projects.	Ensuring SSH access to VMs is centrally managed by IAM , and not SSH keys stored as project/VM metadata.
Cloud IAM	Domain restricted sharing	Defines the set of members (domains) that can be added to Cloud IAM policies.	Protect against malicious acts and human mistakes by ensuring access only for users in whitelisted domains .
GCP	Resource location restriction (Beta)	Defines the set of locations where location-based GCP resources can be created.	Compliance with regulations that restrict resources location.
Cloud Storage	Enforce bucket policy only	Requires buckets to use Bucket Policy only where this constraint.	Object-level access policies don't consider bucket-level policy. They are hard to get visibility into, and can become a security risk .

Figure 4.7 – Example organization policy constraints



Figure 4.8 – Organization policy constraints evaluation criteria

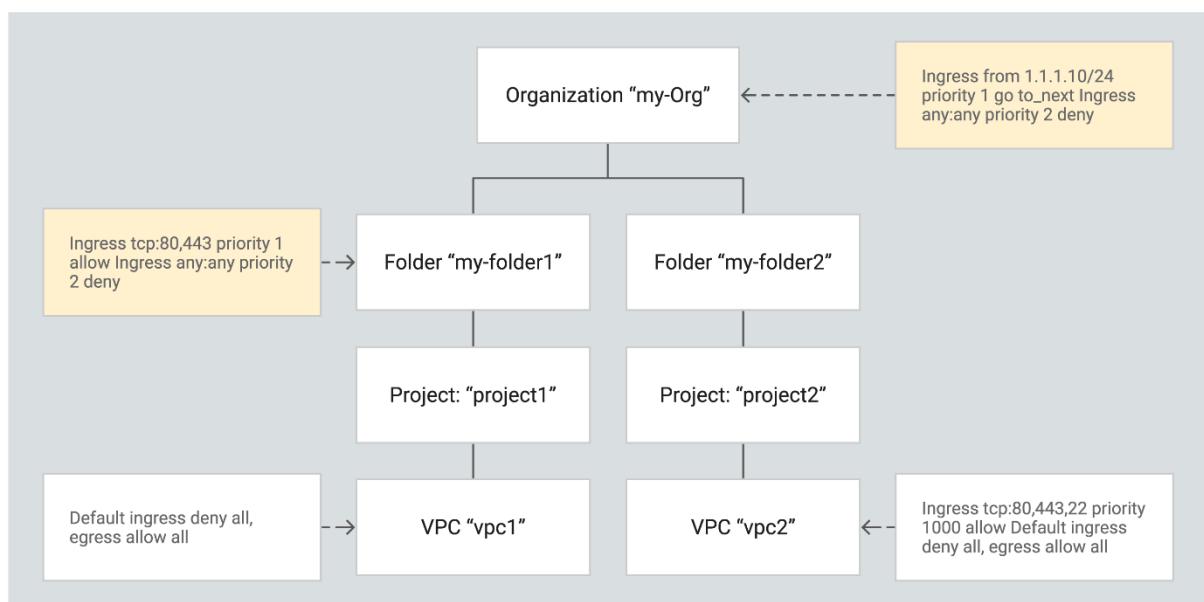


Figure 4.9 – Hierarchical firewall policy inheritance

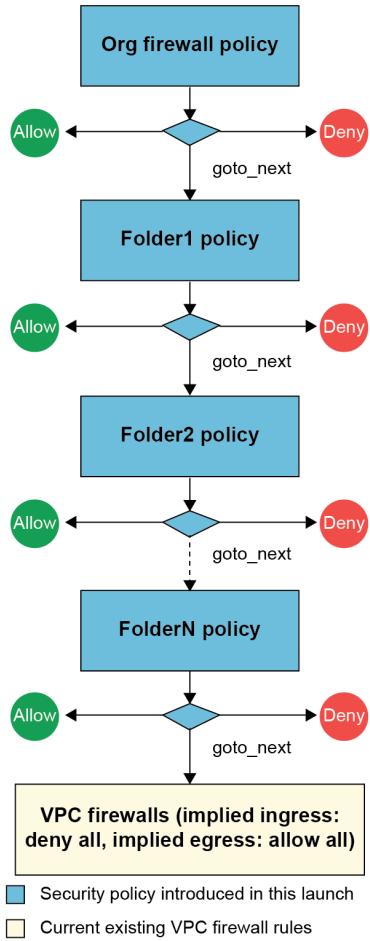


Figure 4.10 – Hierarchical firewall policy evaluation

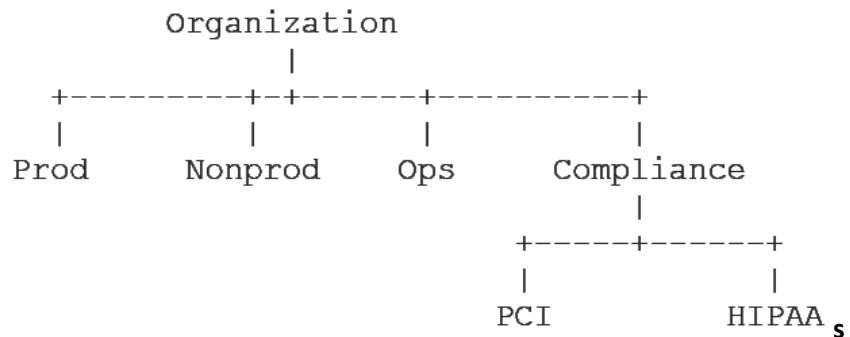


Figure 4.11 – Example organization structure

Chapter 5: Understanding Google Cloud Identity

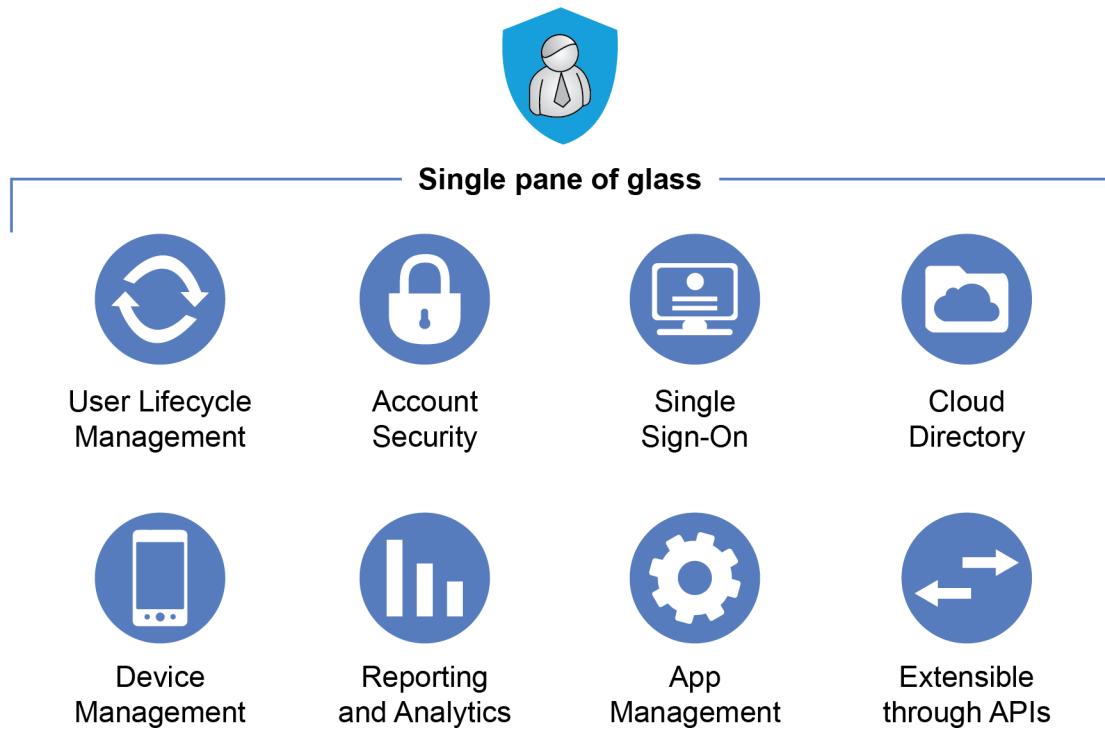


Figure 5.1 – Google Cloud Identity features

The screenshot shows the '2-Step Verification' settings page under 'Security'. On the left, there's a sidebar with 'Organizational Units' and 'Groups' sections. The main area is titled 'Authentication' and is described as 'Locally applied'. It includes the following configuration options:

- Allow users to turn on 2-Step Verification:** A checked checkbox.
- Enforcement:** A radio button set to 'On'.
- New user enrollment period:** A dropdown menu set to 'None'.
- Frequency:** A section where users can avoid repeated 2-Step Verification at login on their trusted devices. A checked checkbox for 'Allow user to trust the device' is present.
- Methods:** A section for selecting the method to enforce. A radio button set to 'Any'.
- 2-Step Verification policy suspension grace period:** A note explaining the grace period for users who temporarily sign in with verification codes.

Figure 5.2 – Account security (2SV)

User information

This user profile is incomplete. Add contact information for Test, like a secondary email address and a phone number.

User details

Security

2-step verification: OFF
Enforced but not enabled for Test

Application-specific password
0 application-specific passwords created

Connected applications
0 applications are connected with Test's account

Recovery information
Add a recovery email
Add a recovery phone

Password settings | Application integrations

Groups

Test doesn't belong to any groups. Add Test to team and project groups, making it easier for this user to collaborate.

Admin roles and privileges

Test doesn't have any admin roles or privileges.

[ASSIGN ROLES](#)

Apps

Google apps
54 of 57 available Google services are on for Test. [Turn apps on or off](#)

Other cloud apps
No other cloud apps have been added to this organization. [Browse for apps](#) [Turn apps on or off](#)

Managed devices

Your organization doesn't have mobile device management.

Figure 5.3 – Cloud Identity – user details

Security

>Password settings

Password Reset Test's password.

Security keys Test has no security keys. [Learn more](#)

Advanced Protection OFF Once you turn off Advanced Protection enrollment, only the user can re-enroll. [Learn more](#)
Trouble signing in Use a backup code for users who are unable to use their security key to sign in. Get a backup code from the 2-Step Verification card.

2-step verification OFF | Enforced across your organization The ability for users to sign in with an additional authentication factor, in addition to using their username and password (e.g. a verification code). [Change security settings](#)
Only the user can turn on 2-step verification. [Learn more](#)
Get backup verification codes

Recovery information Email [Add a recovery email](#)
Phone [Add a recovery phone](#)
Recovery information is used to secure user accounts at sign-in and during account recovery.

Require password change ON This password will need to be changed once Test signs in.

Login challenge Turn off identity questions for 10 minutes after a suspicious attempt to sign in. [Learn more](#)

Sign in cookies Resets the user's sign-in cookies, which also signs them out of their account across all devices and browsers.

Figure 5.4 – Cloud Identity – user security settings

The screenshot shows the 'Google Cloud session control' settings page. At the top, it says 'Google Cloud console and SDK session control' and 'Applied at 'Cloud Sales (ankush)''. A blue info box says 'Use both Google session control and Google Cloud session control to secure access to both web and Cloud platform services.' Below this, the 'Reauthentication policy' section has 'Never require reauthentication' selected. The 'Reauthentication frequency' is set to '1 hour'. The 'Reauthentication method' section has 'Password' selected. A note says 'Most changes take effect in a few minutes. Learn more' and 'You can view prior changes in the Audit log'. At the bottom right are 'CANCEL' and 'SAVE' buttons.

Figure 5.5 – Google Cloud session control

The screenshot shows the 'App access control' settings page under 'API controls'. It says 'Manage app access to your Google services. Ensure that users can give access only to apps that your organisation trusts. Learn more'. The 'Overview' section shows '0 restricted Google services', '15 unrestricted Google services', '2 accessed apps', and buttons for 'MANAGE GOOGLE SERVICES' and 'MANAGE THIRD-PARTY APP ACCESS'. The 'Settings' section has a message 'Show this message if a user tries to use an app that can't access restricted Google services'. Below it is a message input field and two checkboxes: 'Block all third-party API access' (unchecked) and 'Trust internal, domain-owned apps' (checked). A note says 'Internal, domain-owned apps will be exempt from accessing OAuth scopes that are restricted or blocked.' At the bottom, it says 'Apps you trust on the Google Workspace Marketplace, Android, or iOS allowlist are automatically trusted on your App access control list.'

Figure 5.6 – Managing trusted third-party applications

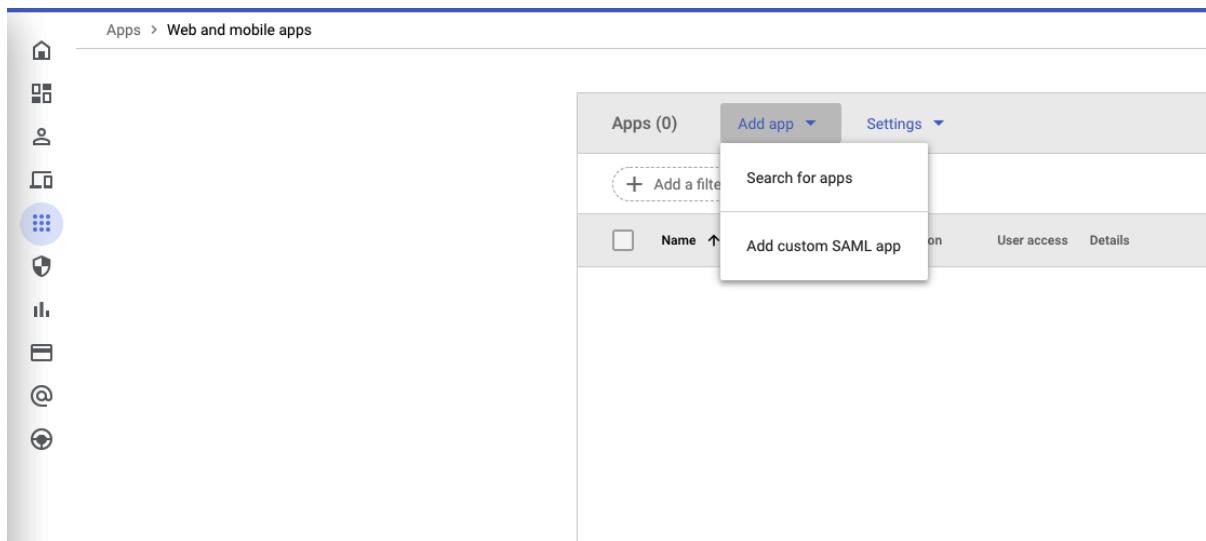


Figure 5.7 – Cloud Identity – Add custom SAML app

A screenshot of the 'Add custom SAML app' configuration page. The title bar says 'Add custom SAML app'. Below it, a progress bar shows step 1 'App details' is active, followed by 'Google Identity Provider detail', 'Service provider details', and 'Attribute mapping'.

App details
Enter details for your custom SAML app. This information is shared with app users. [Learn more](#)

App name
Test Application

Description
A brief description can optionally go here.

App icon
Attach an app icon. Maximum upload file size: 4 MB

[CANCEL](#) [CONTINUE](#)

Figure 5.8 – Configure your custom SAML app

X Add custom SAML app

App details — Google Identity Provider detail: — 3 Service provider details — 4 Attribute mapping

Service provider details

To configure single sign on, add service provider details such as ACS URL and entity ID. [Learn more](#)

ACS URL

Entity ID

Start URL (optional)

Signed response

Name ID

Defines the naming format supported by the identity provider. [Learn more](#)

Name ID format

Name ID
[Basic Information > Primary email](#)

BACK **CANCEL** **CONTINUE**

Figure 5.9 – SAML service provider details

Google Admin Search for users, groups or settings

Apps > Web and mobile apps > **Test Application**

SAML

Test Application

A brief description can optionally go here.

TEST SAML LOGIN

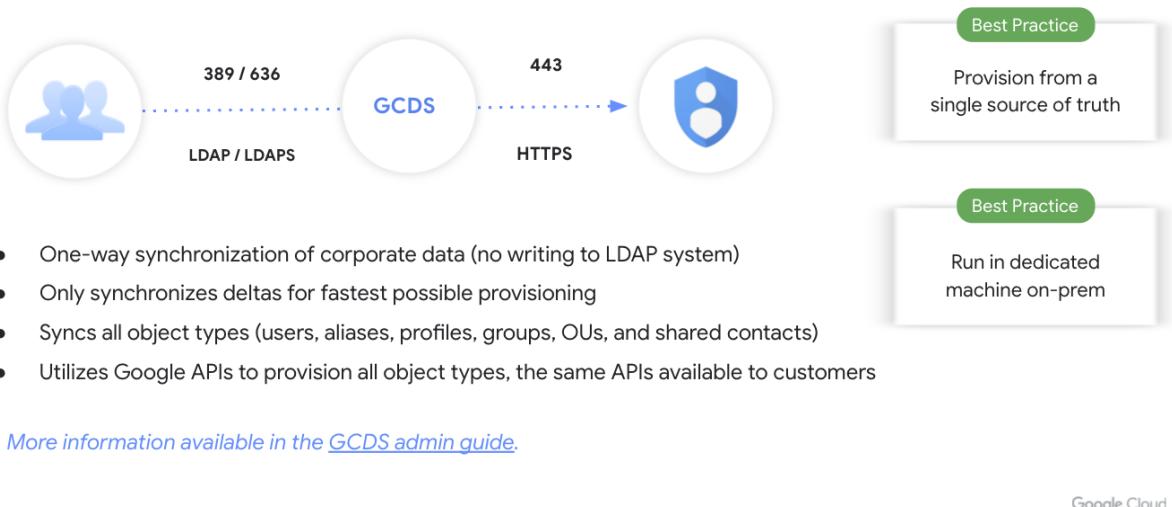
User access
To make the managed app available to select users, choose a group or organizational unit. [Learn more](#)
[View details](#)
OFF for everyone

Service provider details

Certificate Google_2026-6-6-101957_SAML2_0 (Expires Jun 6, 2026)	ACS URL https://example.com/o/saml2/idp?idpid=C045so4hb	Entity ID https://example.com/o/saml2?idpid=C045so4hb
--	--	--

SAML attribute mapping
SAML attribute mapping isn't configured
Map Google directory user profile fields to SAML service provider attributes.
[Configure SAML attribute mapping](#)

Figure 5.10 – App details page



Google Cloud

Figure 5.11 – The workings of GCDS

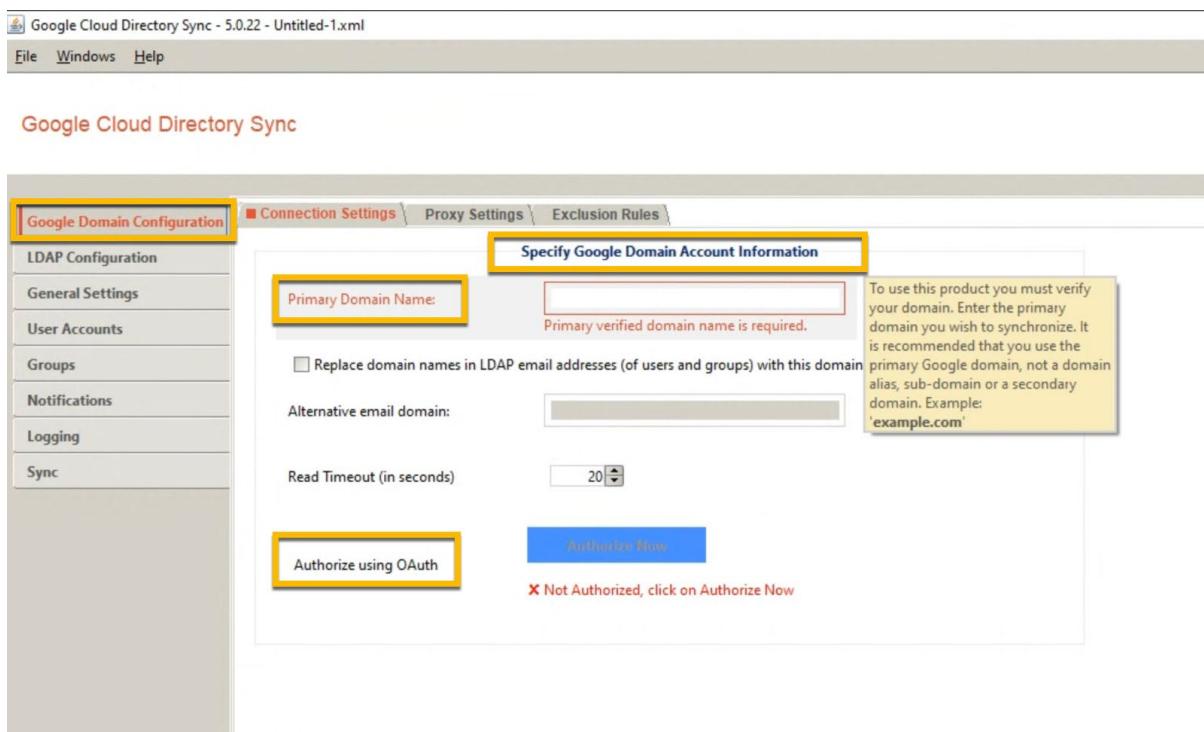


Figure 5.12 – Google Domain configuration

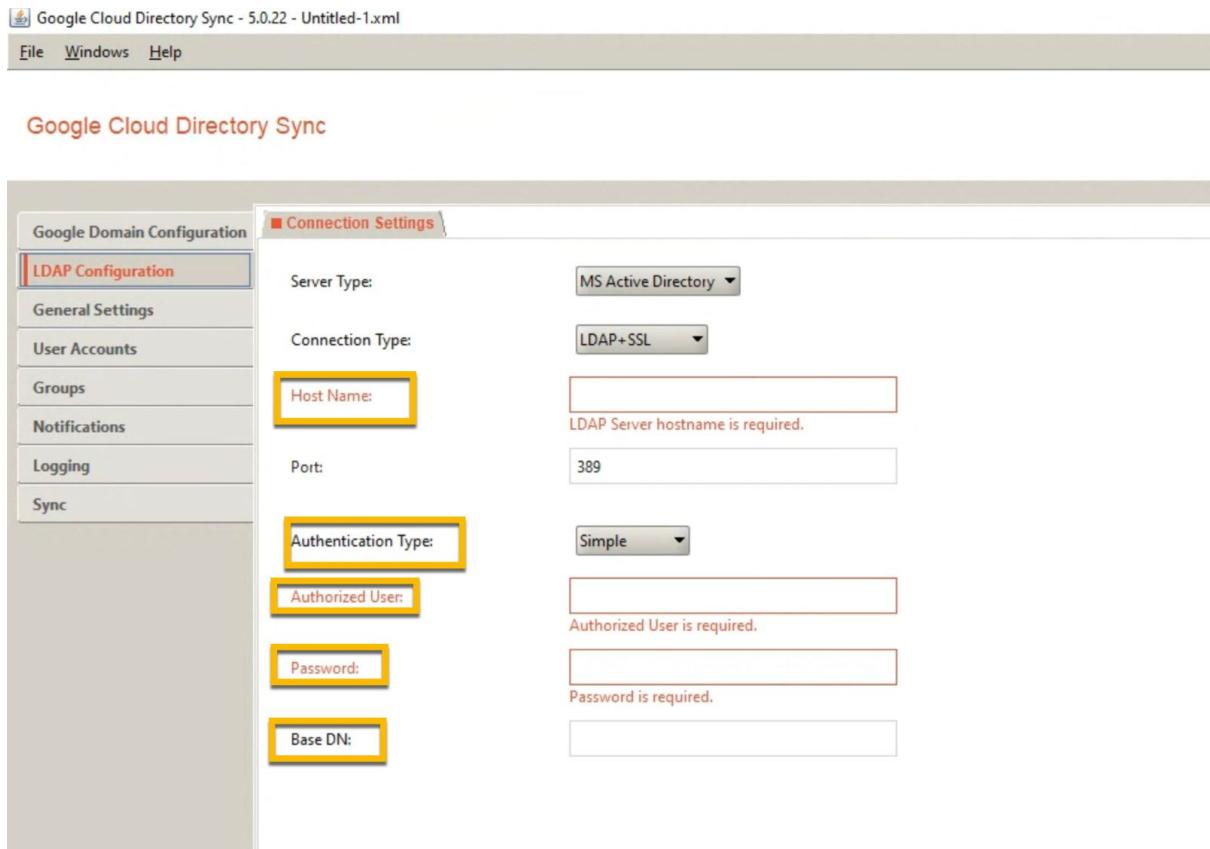


Figure 5.13 – LDAP configuration

Method	Effort	Staff involved	Notes
Manual Provisioning	High	Google Admin	Easiest method, but not scalable
CSV Upload via Google Admin	Medium	Google Admin	More flexibility, but not scalable
Google Cloud Directory Sync (GCDS)	Medium	LDAP Admin	Integrates with LDAP, scalable, requires no programming
Third-Party Tools (Okta, Ping, etc.)	Medium	LDAP Admin	Scalable, may incur additional cost
Admin SDK Directory API	High	LDAP Admin Development Staff	Scalable, flexible, requires in-depth programming

Figure 5.14 – User provisioning options in Google Cloud Identity

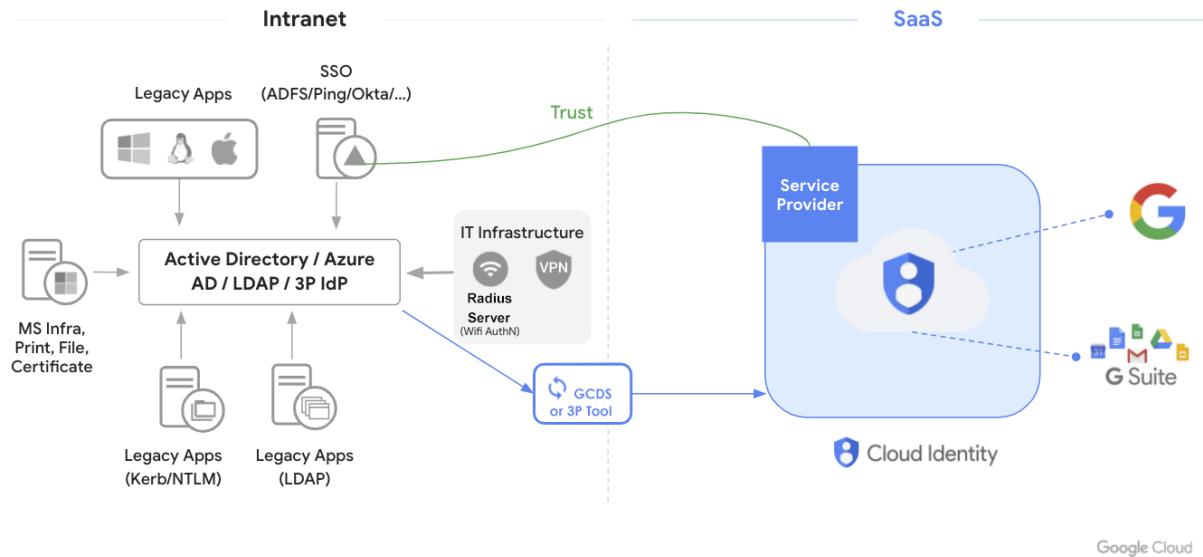


Figure 5.15 – Third party as an IdP



Figure 5.16 – Cloud Identity replicates Bob's identity to all allowed cloud apps



Figure 5.17 – On Bob's first day, he can sign in to all cloud apps using SSO

Chapter 6: Google Cloud Identity and Access Management

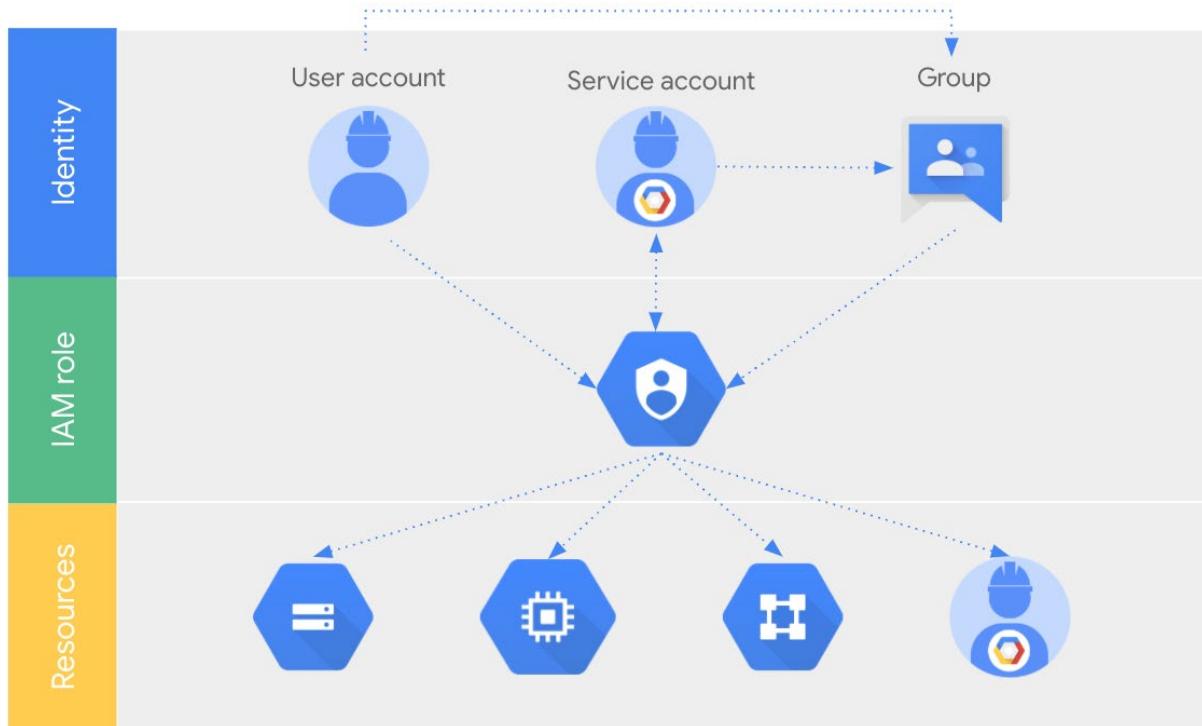


Figure 6.1 – IAM overview

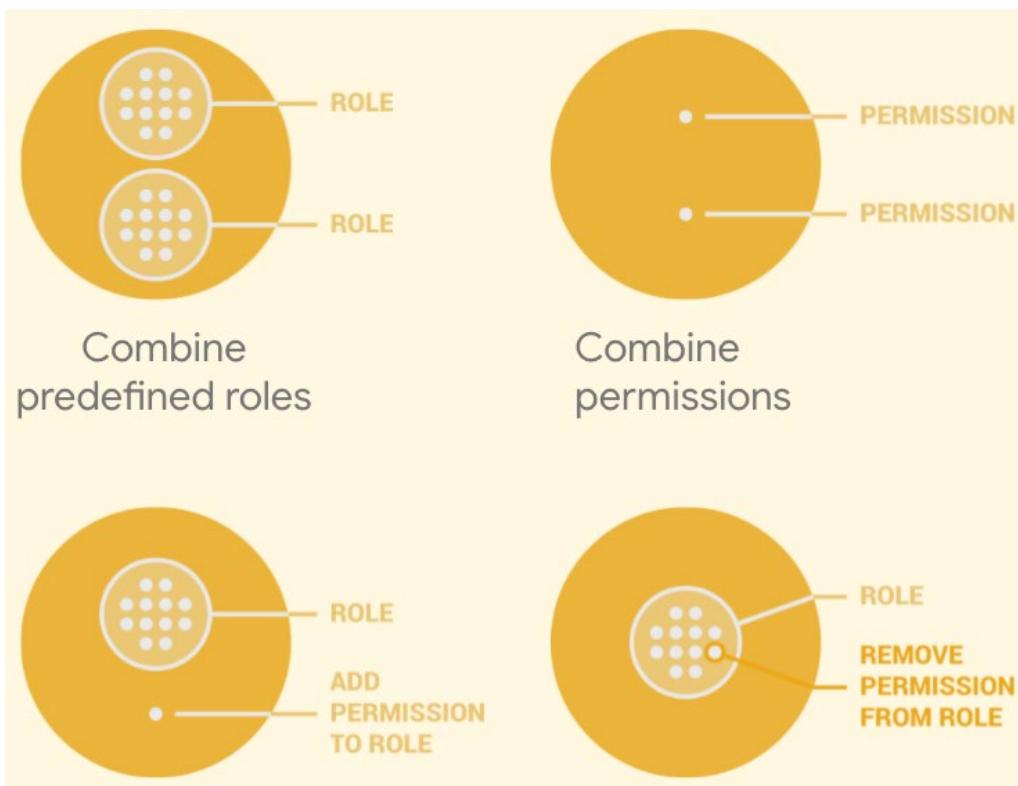


Figure 6.2 – IAM—custom roles

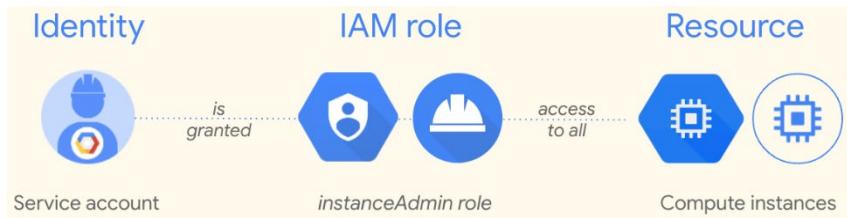


Figure 6.3 – Service account and resource

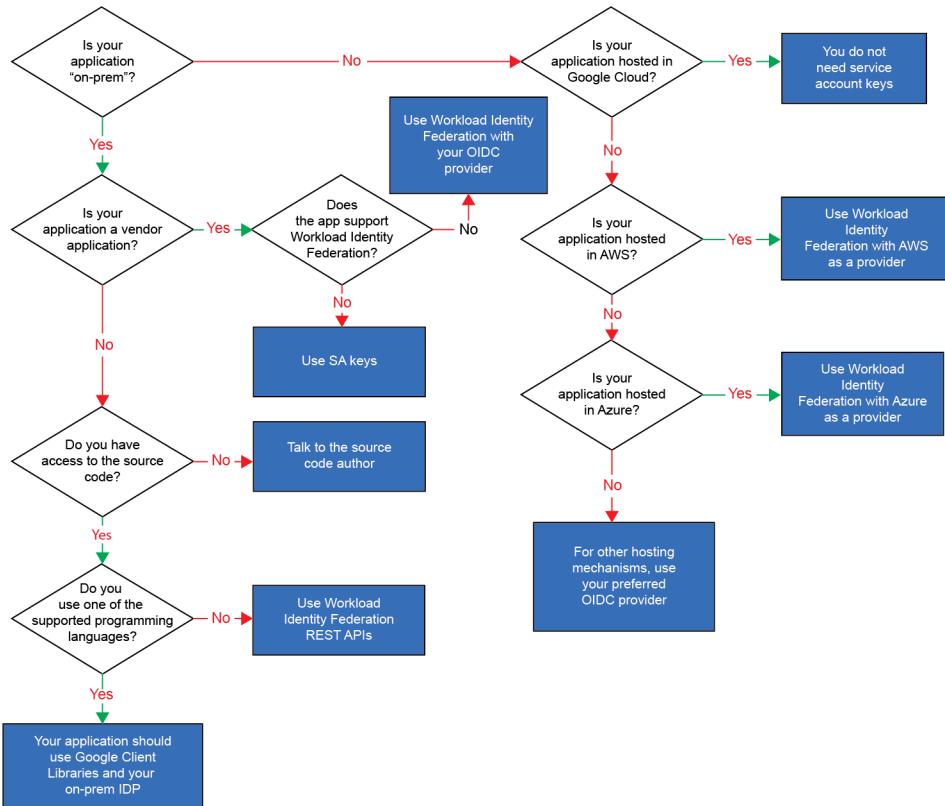


Figure 6.4 – Decision tree for service account keys

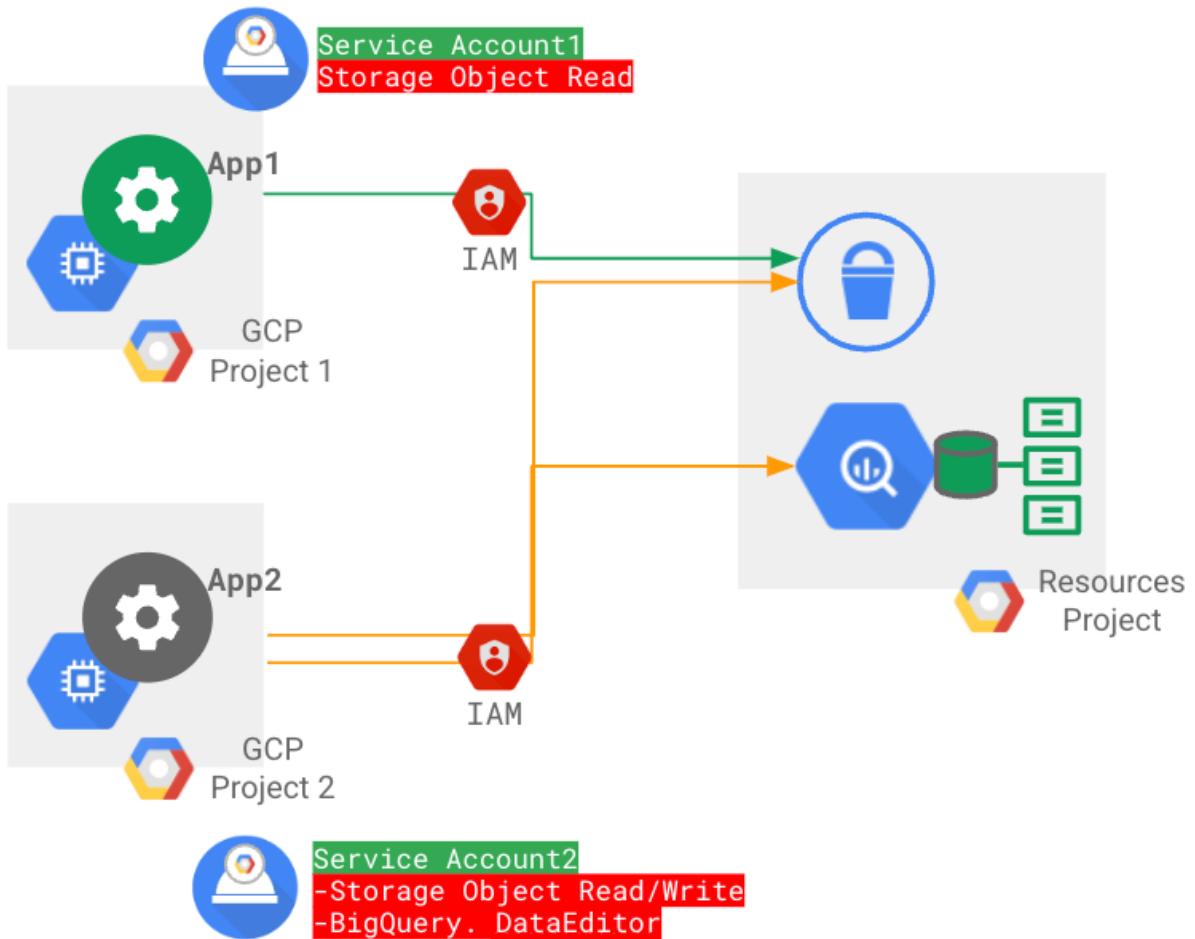


Figure 6.5 – Cross-project service account access

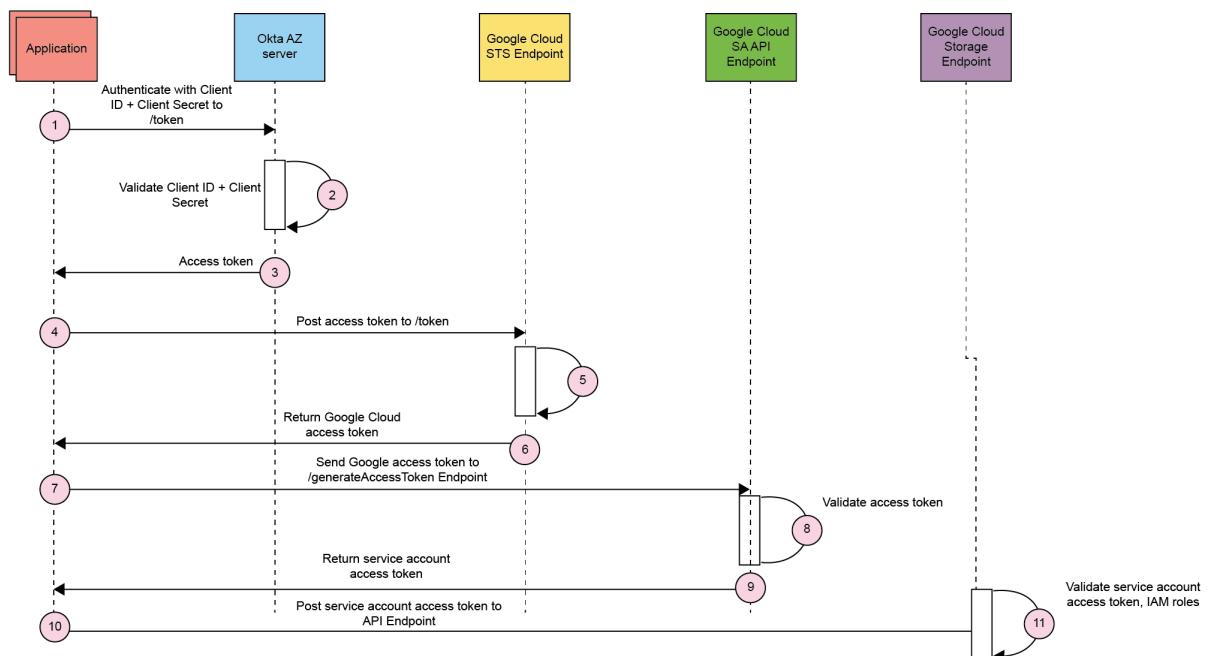


Figure 6.6 – Data flow for WIF with Okta

Chapter 7: Virtual Private Cloud

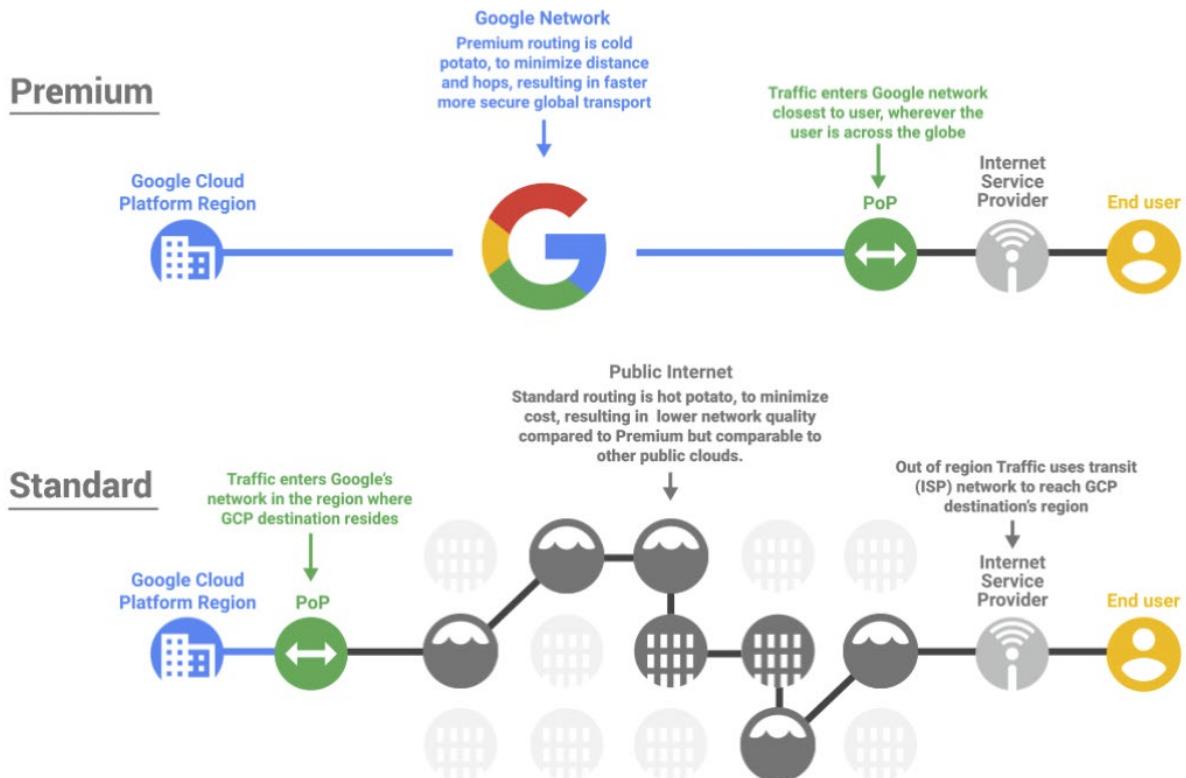


Figure 7.1 – Google Cloud network tiers

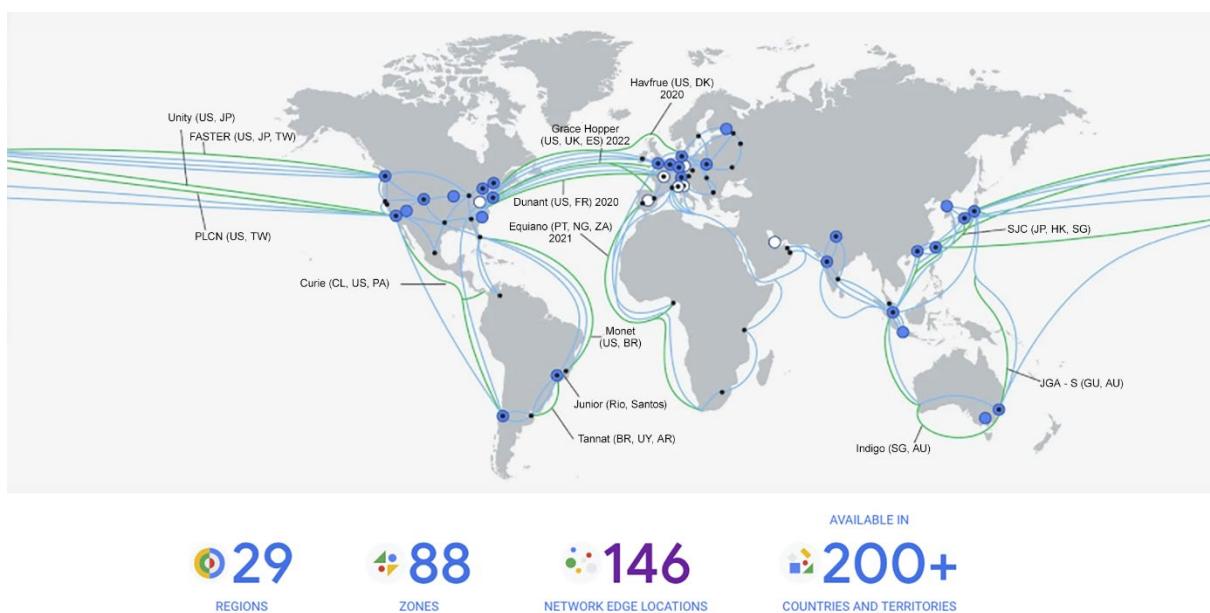


Figure 7.2 – Google Cloud region locations

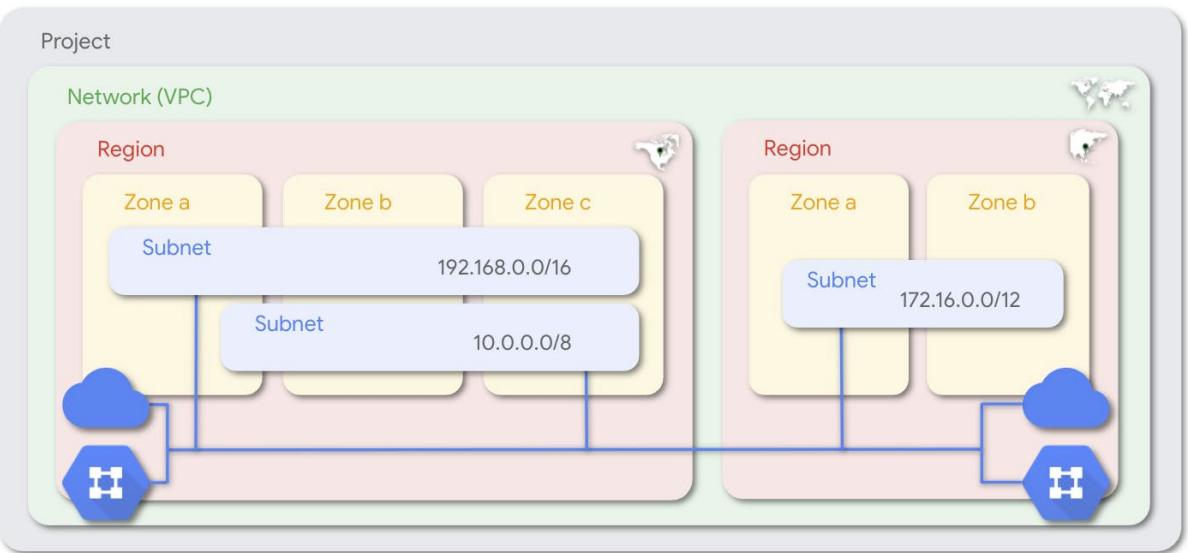


Figure 7.3 – Google network components

[Create a VPC network](#)

Name *



Lowercase letters, numbers, hyphens allowed

Description

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Subnet creation mode

- Custom
 Automatic



These IP address ranges will be assigned to each region in your VPC network. When an instance is created for your VPC network, it will be assigned an IP from the appropriate region's address range.

Region ↑	IP address range
asia-east1	10.140.0.0/20
asia-northeast1	10.146.0.0/20
asia-south1	10.160.0.0/20
asia-southeast1	10.148.0.0/20
australia-southeast1	10.152.0.0/20
europe-west1	10.132.0.0/20
europe-west2	10.154.0.0/20
europe-west3	10.156.0.0/20
europe-west4	10.164.0.0/20
northamerica-northeast1	10.162.0.0/20

Rows per page: 10 ▾

1 – 10 of 15 < >

Figure 7.4 – VPC creation – auto mode

Firewall rules

Select any of the firewall rules below that you would like to apply to this VPC network. Once the VPC network is created, you can manage all firewall rules on the Firewall rules page.

IPV4 FIREWALL RULES		IPV6 FIREWALL RULES						
<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	↑
<input type="checkbox"/>	auto-network-allow-custom 	Ingress	Apply to all	IP ranges: 10.128.0.0/9	all	Allow	65,534	EDIT
<input type="checkbox"/>	auto-network-allow-icmp 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534	
<input type="checkbox"/>	auto-network-allow-rdp 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534	
<input type="checkbox"/>	auto-network-allow-ssh 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65,534	
	auto-network-deny-all-ingress 	Ingress	Apply to all	IP ranges: 0.0.0.0/0	all	Deny	65,535	
	auto-network-allow-all-egress 	Egress	Apply to all	IP ranges: 0.0.0.0/0	all	Allow	65,535	

Figure 7.5 – Default firewall rules

[←](#) Create a VPC network

CUSTOM NETWORK

Lowercase letters, numbers, hyphens allowed

Description

Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click Automatic to create a subnet in each region, or click Custom to manually define the subnets. [Learn more](#)

Subnet creation mode

Custom

Automatic

Edit subnet

Name * us-east-subnet

Lowercase letters, numbers, hyphens allowed

Description

Region * us-east1

IP address range * 192.168.0.0/24

CREATE SECONDARY IP RANGE

Private Google Access ?

On

Off

Flow logs

Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Cloud Logging. [Learn more](#)

On

Off

DONE

ADD SUBNET

Figure 7.6 – Custom VPC creation

Dynamic routing mode ?

Regional

Cloud Routers will learn routes only in the region in which they were created

Global

Global routing lets you dynamically learn routes to and from all regions with a single VPN or interconnect and Cloud Router

DNS server policy

No server policy



Maximum transmission unit (MTU)

1460



CREATE

CANCEL

Figure 7.7 – Dynamic routing

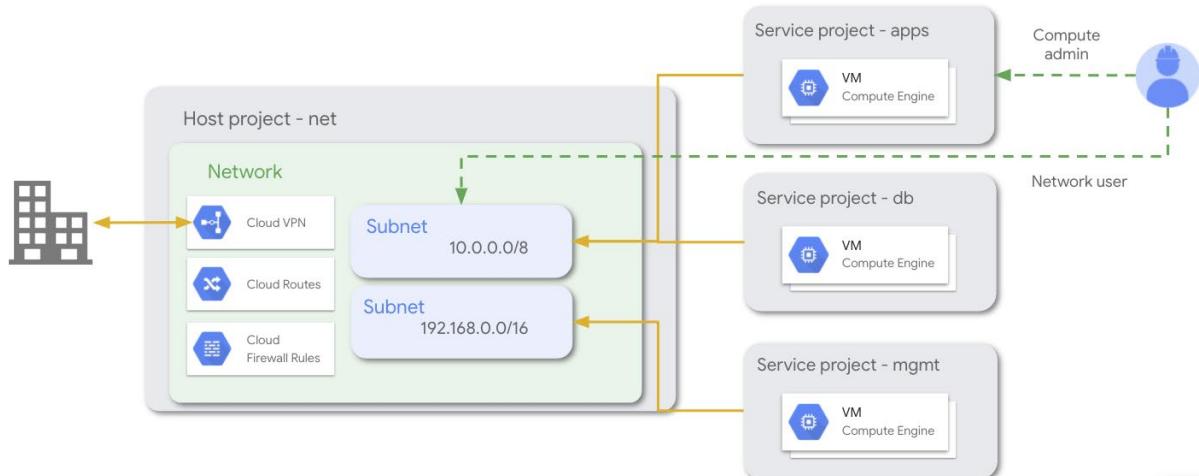


Figure 7.8 – Shared VPC network

Add principals to "exomoon"

Add principals, roles to "exomoon" project

Enter one or more principals below. Then select a role for these principals to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New principals —

X ?

Role *	Condition	Remove
Project IAM Admin	Add condition	█
Access and administer a project IAM policies.		
Role	Condition	Remove
Compute Network Viewer	Add condition	█
Read-only access to Compute Engine networking resources.		
Select a role	Condition	Remove
Select a role	Add condition	█

+ ADD ANOTHER ROLE

SAVE CANCEL

Figure 7.9 – Assign IAM roles for Shared VPC

VPC Network

Shared VPC

Shared VPC lets you share subnets with other projects. You can then create resources (like VM instances) on those subnets. [Learn more](#)

[SET UP SHARED VPC](#)

[MANAGE ALL SHARED VPC](#)

Figure 7.10 – SET UP SHARED VPC

The screenshot shows a web-based configuration interface for setting up a Shared VPC. On the left is a vertical toolbar with icons for various services like Compute Engine, Cloud Storage, and Cloud Functions. The main area has a header 'Set up Shared VPC' with a back arrow. A sidebar on the left lists three steps: 1. Enable host project (selected), 2. Select subnets, and 3. Give permissions. Step 1 contains a sub-step for 'Project ID' which is set to 'starship-289207'. At the bottom are 'SAVE & CONTINUE' and 'CANCEL' buttons.

← Set up Shared VPC

1 Enable host project
This project will become a host project after you click 'Save and continue'. [Learn more](#)

Project ID
starship-289207

SAVE & CONTINUE CANCEL

2 Select subnets

3 Give permissions

Figure 7.11 – Enable host project

2 Select subnets

Select which subnets you want to share. You can share all subnets in this project (including ones created in the future) or select them individually.

Sharing mode

Share all subnets (project-level permissions)

All subnets in this project will be shared, including ones created in the future.

Individual subnets (subnet-level permissions)

Individual subnets you want to share. Subnets created in the future will not be shared automatically.

Subnets to share

Filter subnetworks

<input type="checkbox"/>	Subnet ↑	Region	VPC network	IP addresses range
<input type="checkbox"/>	default	asia-east1	default	10.140.0.0/20
<input type="checkbox"/>	default	asia-east2	default	10.170.0.0/20
<input type="checkbox"/>	default	asia-northeast1	default	10.146.0.0/20
<input type="checkbox"/>	default	asia-northeast2	default	10.174.0.0/20
<input type="checkbox"/>	default	asia-northeast3	default	10.178.0.0/20
<input type="checkbox"/>	default	asia-south1	default	10.160.0.0/20
<input type="checkbox"/>	default	asia-south2	default	10.190.0.0/20
<input type="checkbox"/>	default	asia-southeast1	default	10.148.0.0/20
<input type="checkbox"/>	default	asia-southeast2	default	10.184.0.0/20
<input type="checkbox"/>	default	australia-southeast1	default	10.152.0.0/20

0 subnets will be shared

[CONTINUE](#)

[CANCEL](#)

Figure 7.12 – Select subnets

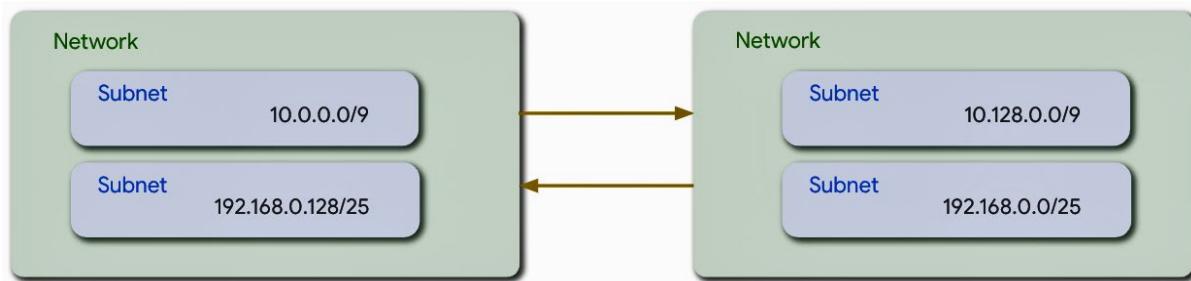


Figure 7.13 – VPC peering



← Create peering connection

ⓘ Your VPC network will be fully connected to the peered VPC network (full mesh topology). Routes to subnets in the peered VPC network will be automatically created.

Name * ?

Lowercase letters, numbers, hyphens allowed

Your VPC network * ?

Peered VPC network

- In project starship-289207
 In another project

VPC network name * ?

Exchange custom routes ?

You can choose to import or export static and dynamic routes over the VPC peering connection

- Import custom routes ?
 Export custom routes ?

Exchange subnet routes with public IP ?

You can choose to import or export subnet routes with public IP over the VPC peering connection

- Import subnet routes with public IP ?
 Export subnet routes with public IP ?

CREATE

CANCEL

Figure 7.14 – Create peering connection

	Shared VPC	VPC Peering	Cloud VPN
Network services management (Firewalls, subnets, routes, VPN, DNS)	Central management of shared network resources	Clear network and security administrative boundaries	Clear network and security administrative boundaries
Transitivity	N/A	Non-transitive	Transitive
Scale	1000 service projects or more, depending on multiple factors	Up to 25 peered networks	Approximately 100 connected projects
Pricing	General network pricing	General network pricing	General network pricing. Excluding intra-zone traffic, which is <u>billed</u> as interzone.
Performance implication	None	None	Throughput limited based on number of tunnels (1.5 to 3 Gbps per tunnel)

Figure 7.15 – Cross-project communication options comparisons

	Primary	Secondary
Configuration	Mandatory – one per subnet	Optional – multiple ranges are supported
Used for	Allocation of VM primary IP reserved IPs	Allocating a different IP to multiple microservices running in a VM (e.g., containers, GKE pods).
Extendable	Range can be extended, but not shrunk	No

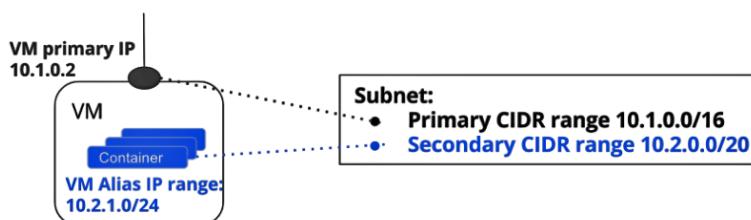


Figure 7.16 – Subnet CIDR ranges

Route	Type	Created by	Next Hop	Restrictions	Exchanged with VPC Peering
Subnet route	System	System	VPC network	Cannot be removed	Automatic
Static route	Custom	User	Instance IP/name Cloud VPN	Must be broader than a subnet IP range	Flag controlled
Dynamic route	Custom	Cloud router (BGP session)	BGP peer	Must be broader than a subnet IP range	Flag controlled

Figure 7.17 – VPC routes

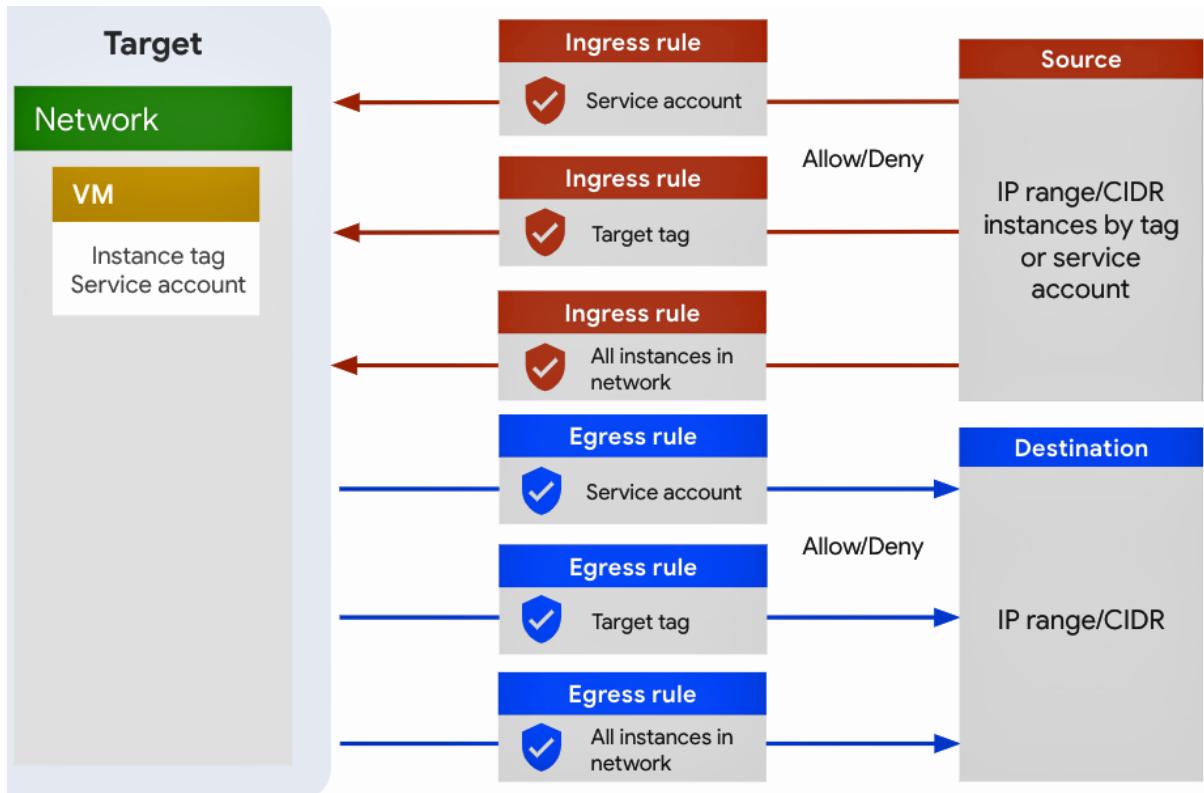


Figure 7.18 – VPC firewall rules

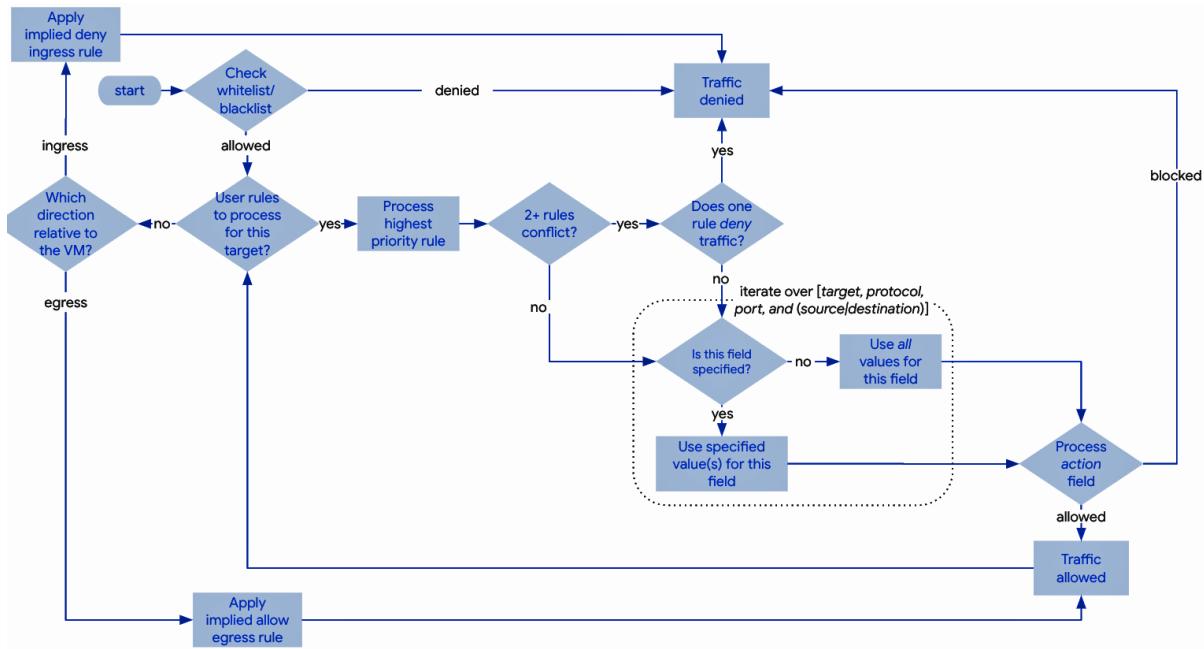


Figure 7.19 – Firewall rule evaluation logic

[←](#) Create a firewall rule

Name *
new-rule-tags [?](#)

Lowercase letters, numbers, hyphens allowed

Description
Some optional description can go here [?](#)

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

On

Off

[▼ SHOW LOGS DETAILS](#)

Network *
vpca [?](#)

Priority *
1000 [CHECK PRIORITY OF OTHER FIREWALL RULES](#) [?](#)

Priority can be 0 - 65535

Direction of traffic [?](#)

Ingress

Egress

Action on match [?](#)

Allow

Deny

Targets

Specified target tags [?](#)

Target tags *

http-server [X](#) web-server [X](#)

Source filter

IPv4 ranges [?](#)

Source IPv4 ranges *

192.168.0.0/24 [X](#) for example, 0.0.0.0/0, 192.168.2.0/24 [?](#)

Second source filter

None [?](#)

Protocols and ports [?](#)

Allow all

Specified protocols and ports

tcp : 80,443

udp : all

Figure 7.20 – Create a firewall rule using target tags

[Create a firewall rule](#)

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name *

new-rule-sa



Lowercase letters, numbers, hyphens allowed

Description

Some optional description can go here

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

On

Off

SHOW LOGS DETAILS

Network *

vpc-a



Priority *

1000

[CHECK PRIORITY OF OTHER FIREWALL RULES](#)



Priority can be 0 - 65535

Direction of traffic

Ingress

Egress

Action on match

Allow

Deny

Targets

Specified service account



Service account scope

In this project

In another project

Target service account

Compute Engine default service account



Figure 7.21 – Create a firewall rule using the service account

≡ Google Cloud Platform • my-project ▾

 [Create a DNS zone](#)

A DNS zone is a container of DNS records for the same DNS name suffix. In Cloud DNS, all records in a managed zone are hosted on the same set of Google-operated authoritative name servers. [Learn more](#)

Zone name [?](#)

DNS name [?](#)

DNSSEC [?](#)

Description (Optional)

Equivalent [REST](#) or [command line](#)

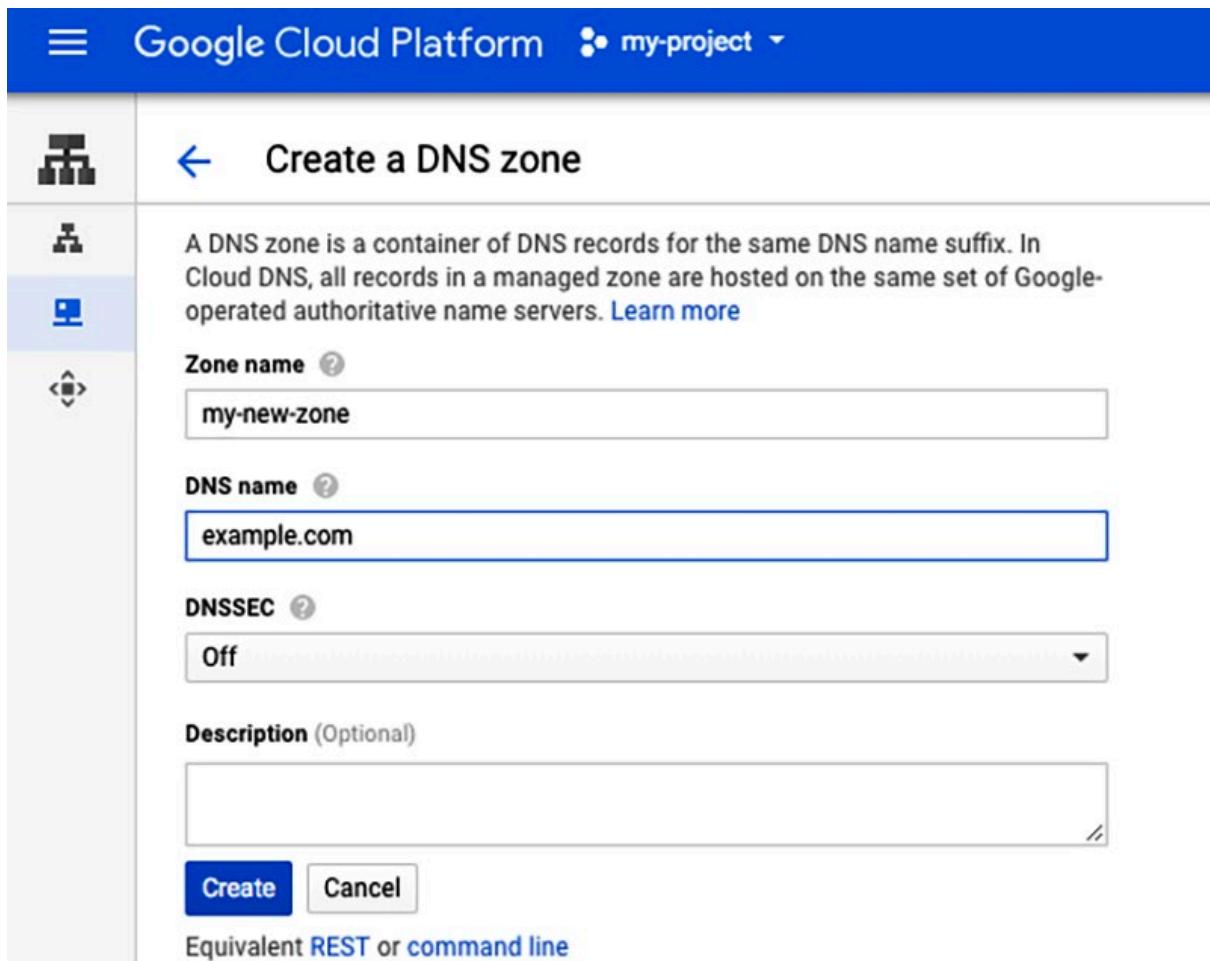


Figure 7.22 – Create a DNS zone

 Network services

 Load balancing

 **Cloud DNS**

 Cloud CDN

 Cloud NAT

 Traffic Director

[← Create record set](#)

DNS Name [?](#)

Resource Record Type [?](#) **TTL** [?](#) **TTL Unit** [?](#)

IPv4 Address [?](#)

Equivalent [REST](#) or [command line](#)

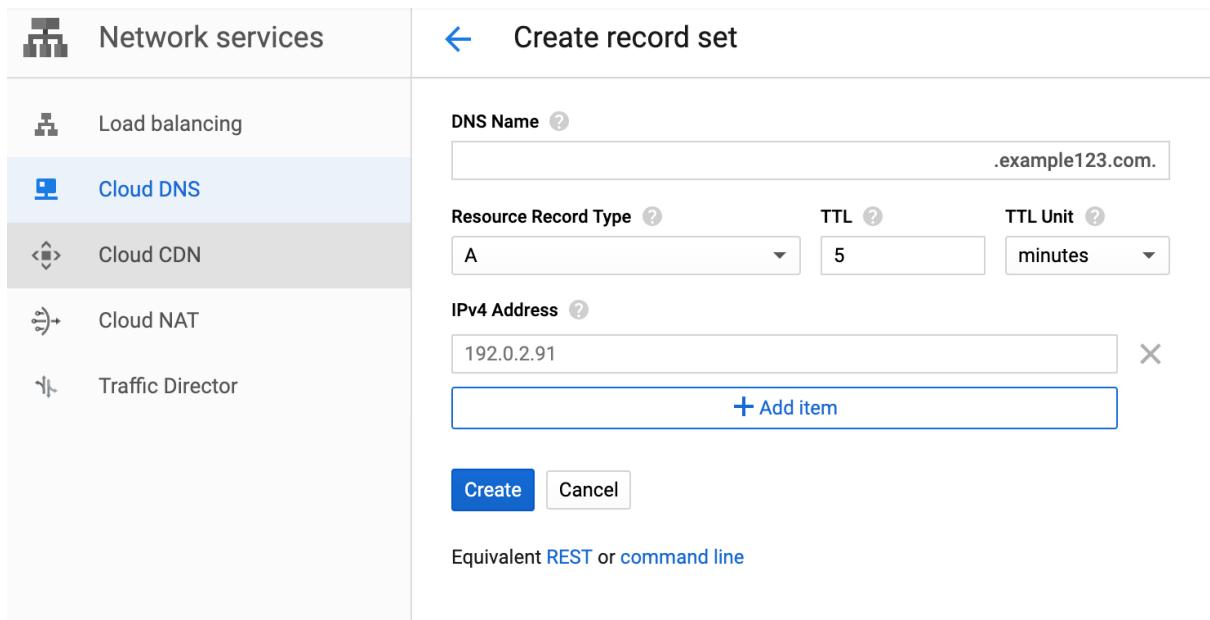


Figure 7.23 – Create a record sets

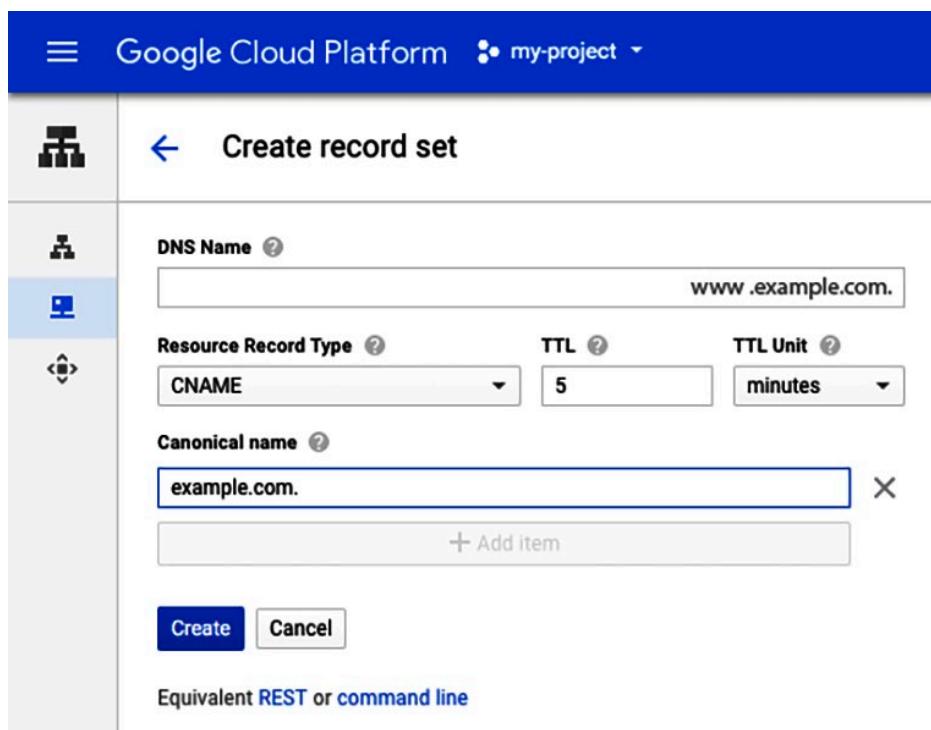


Figure 7.24 – Create a CNAME record

[Create a DNS zone](#)

A DNS zone is a container of DNS records for the same DNS name suffix. In Cloud DNS, all records in a managed zone are hosted on the same set of Google-operated authoritative name servers. [Learn more](#)

If you don't have a domain yet, purchase one through [Cloud Domains](#).

Zone type

- Private
- Public

Zone name *
`secure-private-zone`

Example: example-zone-name

DNS name *
`domain.com`

Example: myzone.example.com

DNSSEC *
On

Description

Cloud Logging

- On
- Off

After creating your zone, you can add resource record sets and modify the networks your zone is visible on.

CREATE

CANCEL

EQUIVALENT COMMAND LINE

Figure 7.25 – Enable DNSSEC for a private DNS zone

	Type	Geographical scope	Network tiers	Proxy/pass-through
Internal	TCP/UDP	Regional	Premium	Pass-through
	HTTP(s)			Proxy
External	TCP/UDP	Regional	Standard/Premium	Pass-through
	HTTP(s)	Regional/Global depending on network tier	Standard/Premium	Proxy
	TCP proxy			
	SSL proxy			

Figure 7.26 – Different types of Google Cloud load balancers

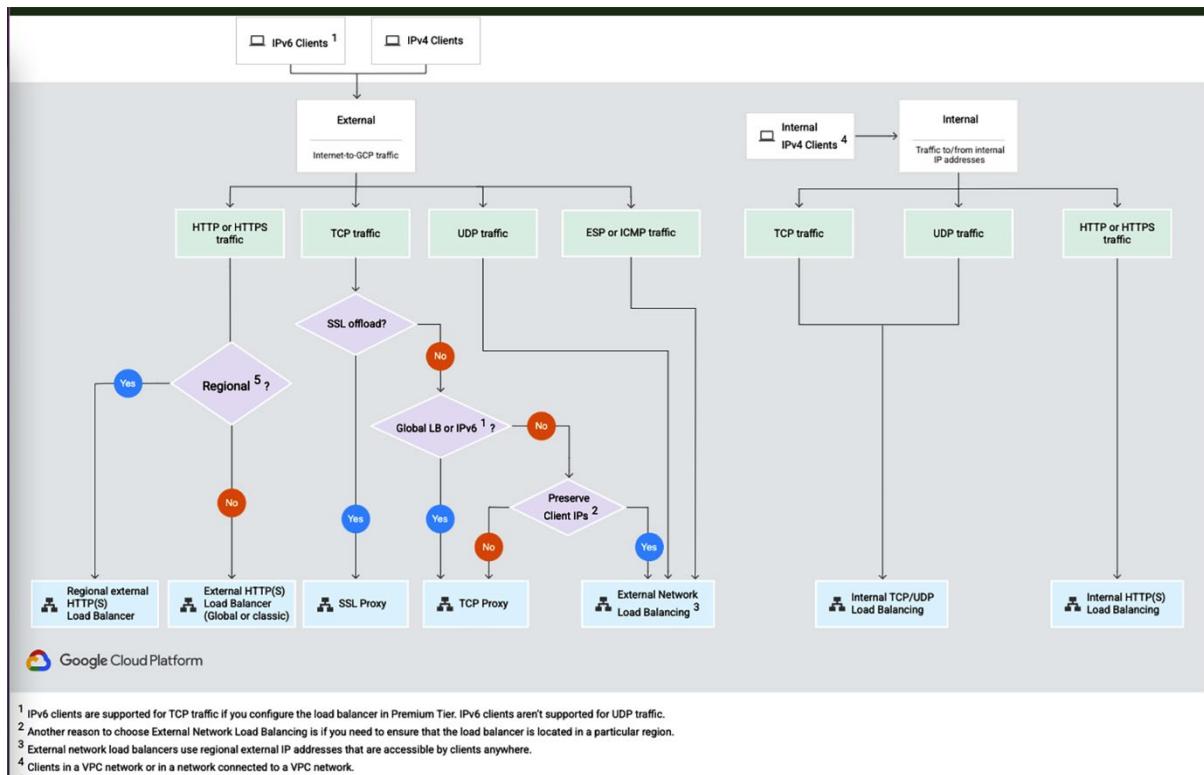


Figure 7.27 – Decision tree for choosing a load balancer

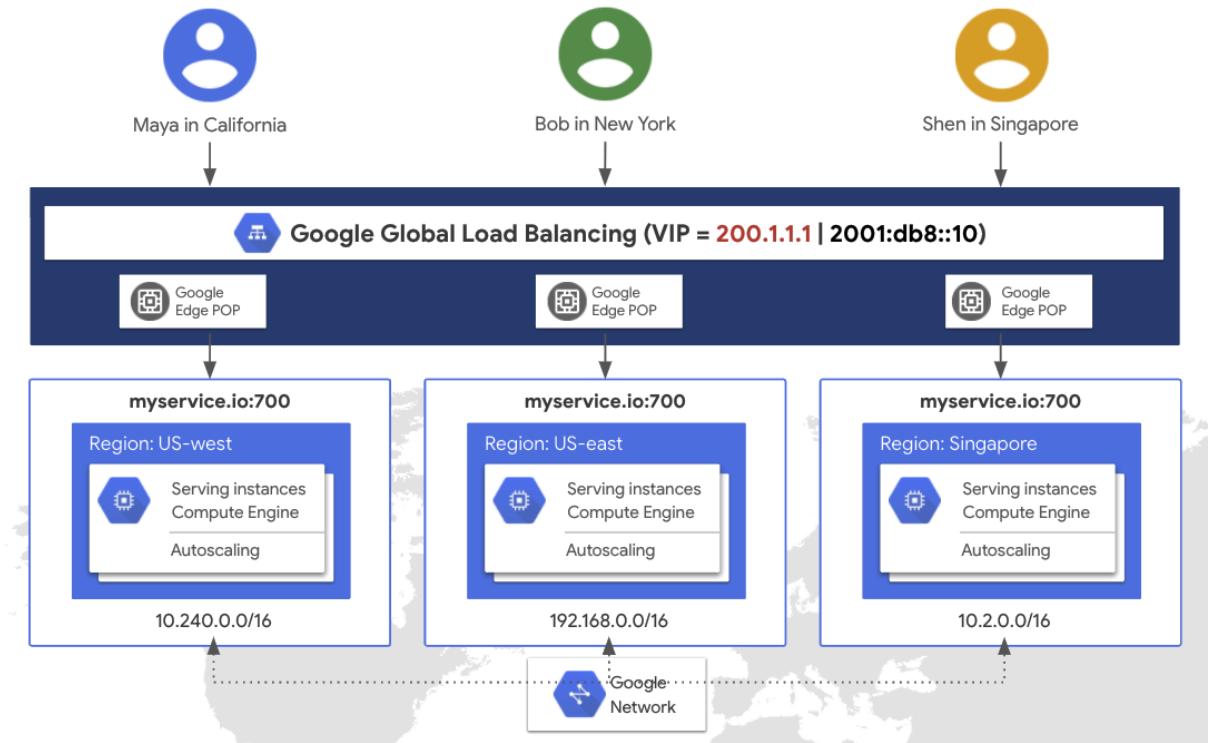


Figure 7.28 – External global HTTP(S) load balancing

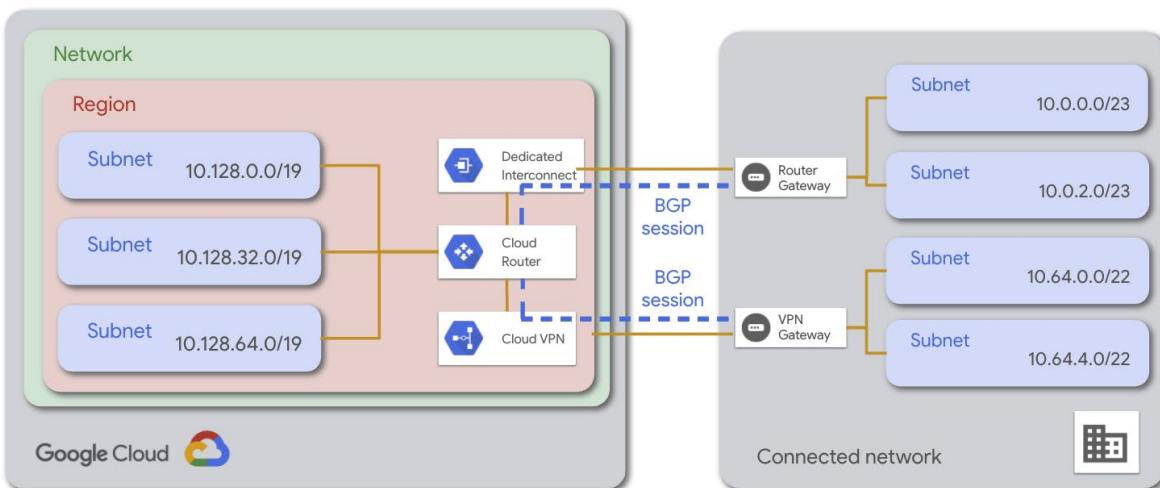


Figure 7.29 – Cloud Router

s

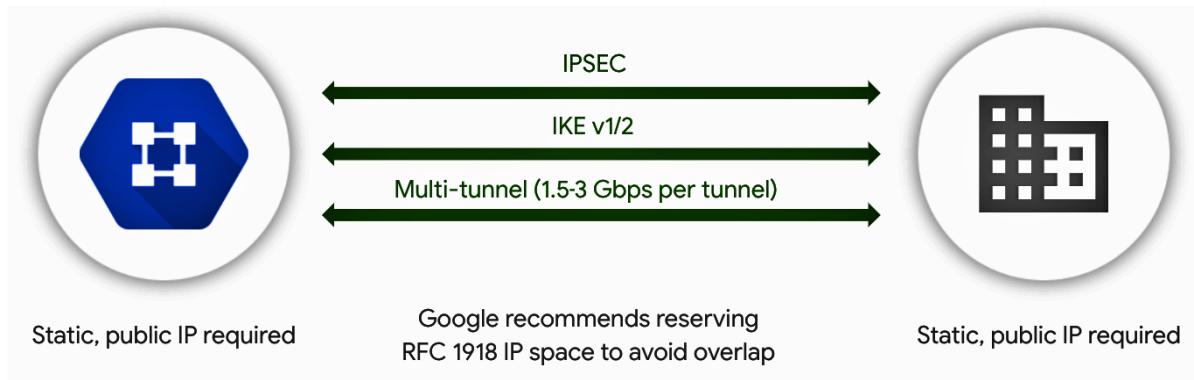


Figure 7.30 – Cloud VPN

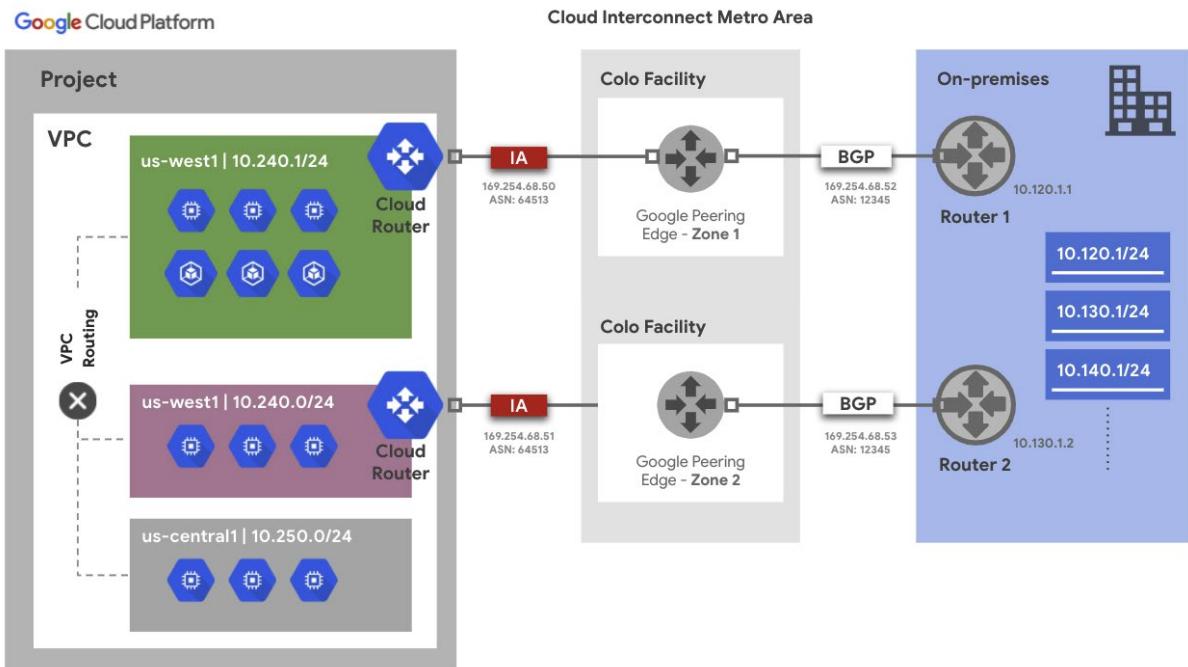


Figure 7.31 – Cloud Interconnect

Chapter 8: Advanced Network Security

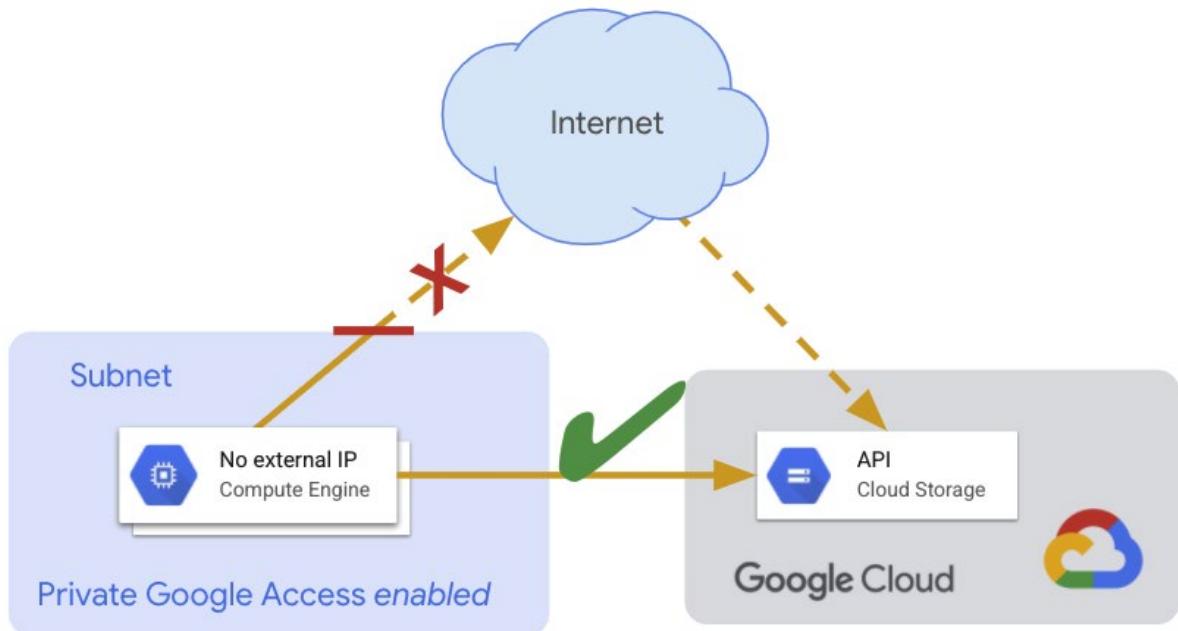


Figure 8.1 – Private Google Access

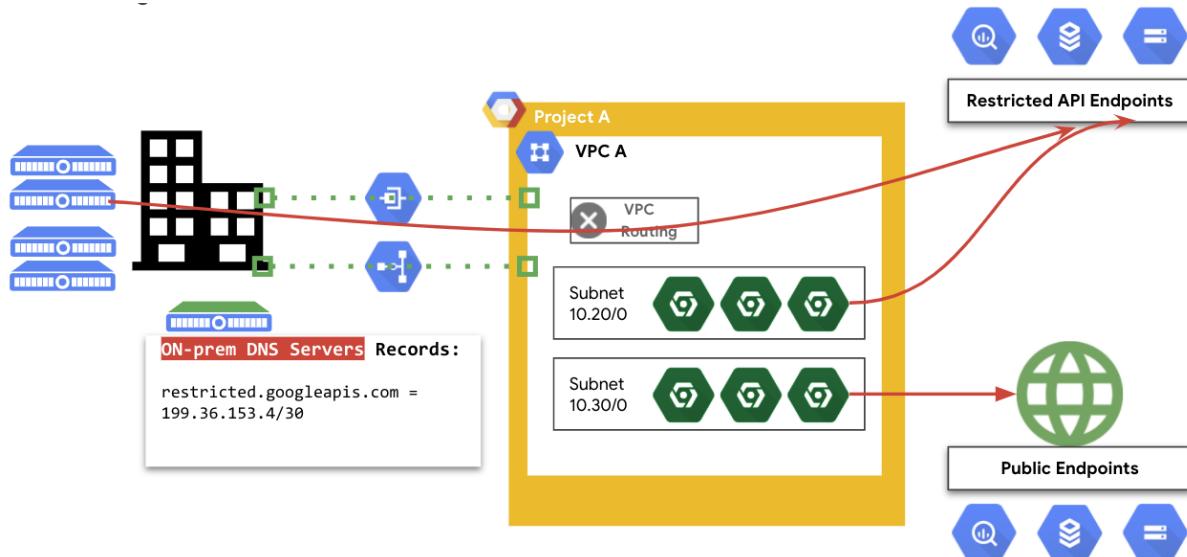


Figure 8.2 – Private Google Access for on-premises services

The screenshot shows the Google Cloud VPC network Routes page. On the left, there's a sidebar with options like VPC networks, IP addresses, Firewall, and Routes (which is selected). The main area shows a table of routes. There's one row for a 'Default route to the Internet' with the following details:

Name	Description	IP version	Destination IP range	Priority	Instance tags	Next hop	Network
default-route-15b9fbc754e9eda9	Default route to the Internet	IPv4	0.0.0.0/0	1000	None	Default internet gateway	default

Figure 8.3 – Default internet gateway route

Create a route

Name *
custom-vpn-route ?

Lowercase letters, numbers, hyphens allowed

Description

//

Network *
default ? ▾

Destination IP range *
E.g. 10.0.0.0/16 ?

Priority *
1000 ?

Priority should be a positive integer (lower values take precedence)

Instance tags ?

Next hop
Specify VPN tunnel ? ▾

VPN tunnel * ? ▾

! VPN Tunnel is required

CREATE **CANCEL**

Figure 8.4 – Create a route for the VPN tunnel

≡ Google Cloud My First Project

VPC network Subnet details EDIT DELETE

VPC networks	new
IP addresses	VPC Network holodeck
Bring your own IP	
Firewall	Region europe-central2
Routes	IP stack type <input checked="" type="radio"/> IPv4 (single-stack) <input type="radio"/> IPv4 and IPv6 (dual-stack) ?
VPC network peering	
Shared VPC	
Serverless VPC access	
Packet mirroring	IP ranges <p>Subnetwork IP ranges must be unique and non-overlapping within a VPC network and peered VPC network. The following ranges are currently being used in other regions: None</p>

IPv4 address range * 192.168.10.0/24

Secondary IPv4 ranges ? + ADD IP RANGE

Gateway 192.168.10.1

Private Google Access
 On
 Off

Flow logs
 On
 Off

SAVE CANCEL EQUIVALENT REST

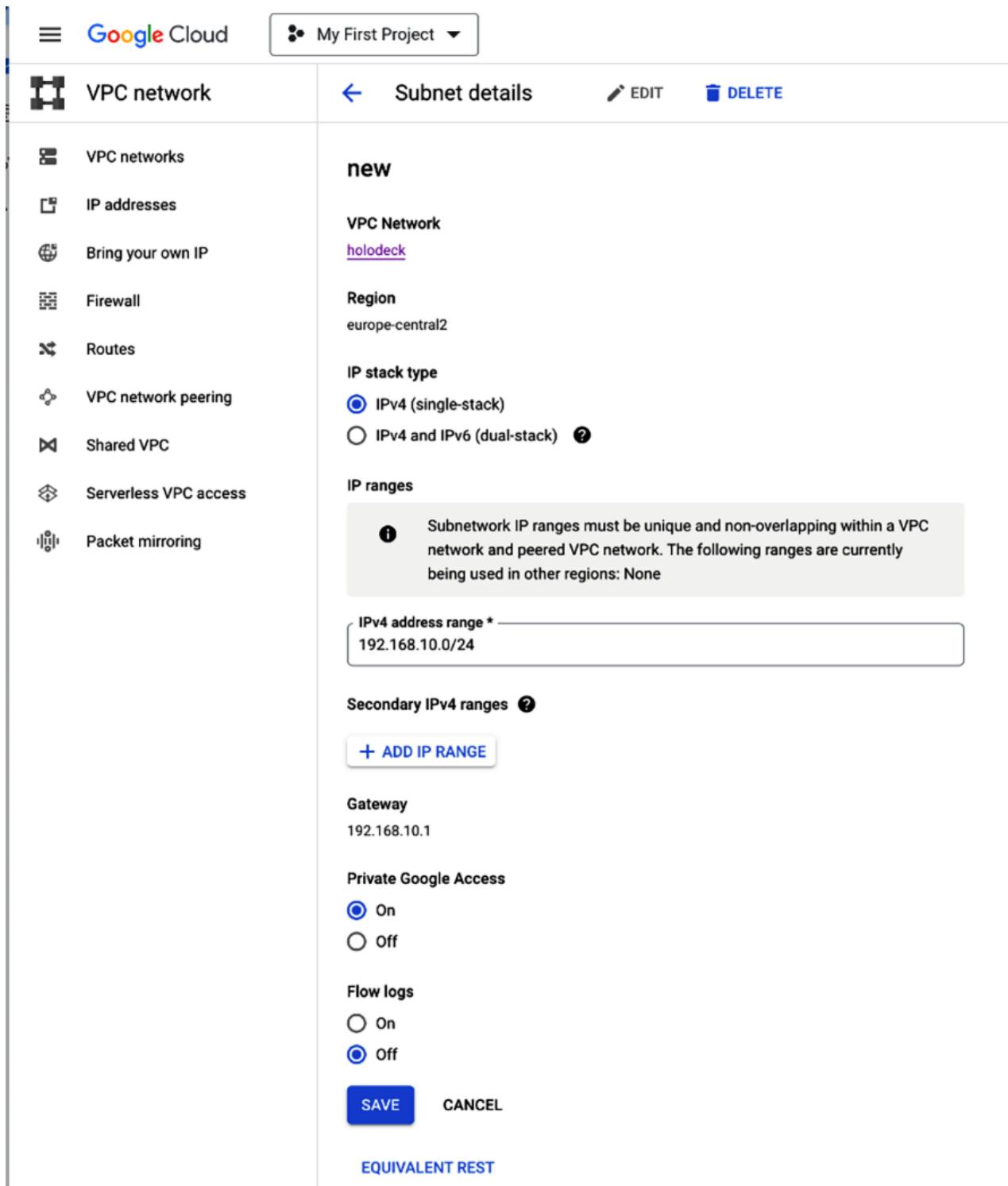


Figure 8.5 – Enable Private Google Access for the subnet

≡ Google Cloud My First Project ▾

VPC network Subnet details EDIT DELETE

new

VPC Network
holodeck

Region
europe-central2

IP stack type
 IPv4 (single-stack)
 IPv4 and IPv6 (dual-stack) ?

IP ranges

i Subnetwork IP ranges must be unique and non-overlapping within a VPC network and peered VPC network. The following ranges are currently being used in other regions: None

IPv4 address range *
192.168.10.0/24

Secondary IPv4 ranges ?
+ ADD IP RANGE

Gateway
192.168.10.1

Private Google Access
 On
 Off

Flow logs
 On
 Off

SAVE CANCEL

EQUIVALENT REST

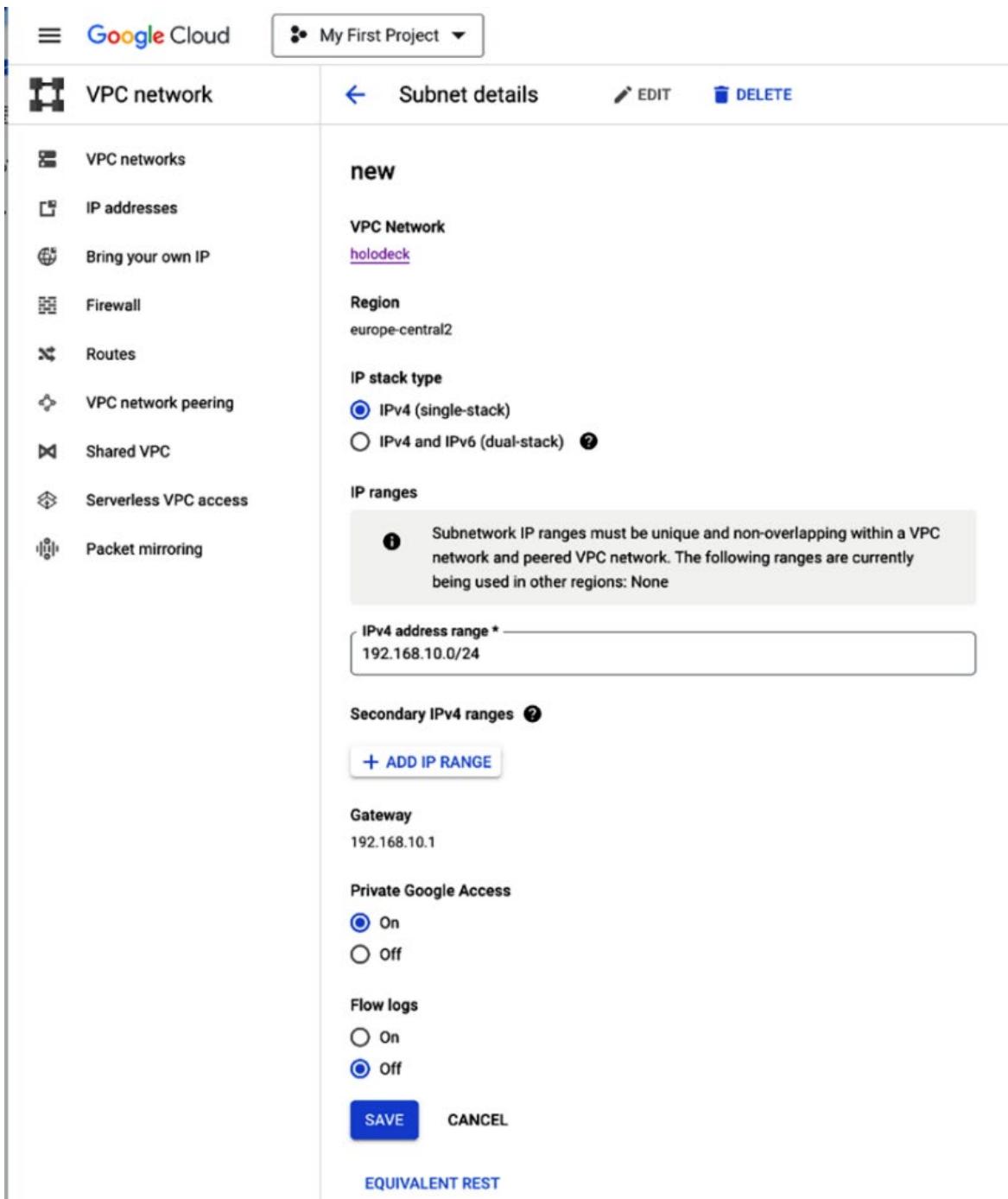


Figure 8.6 – Configuring subnet for Private Google Access

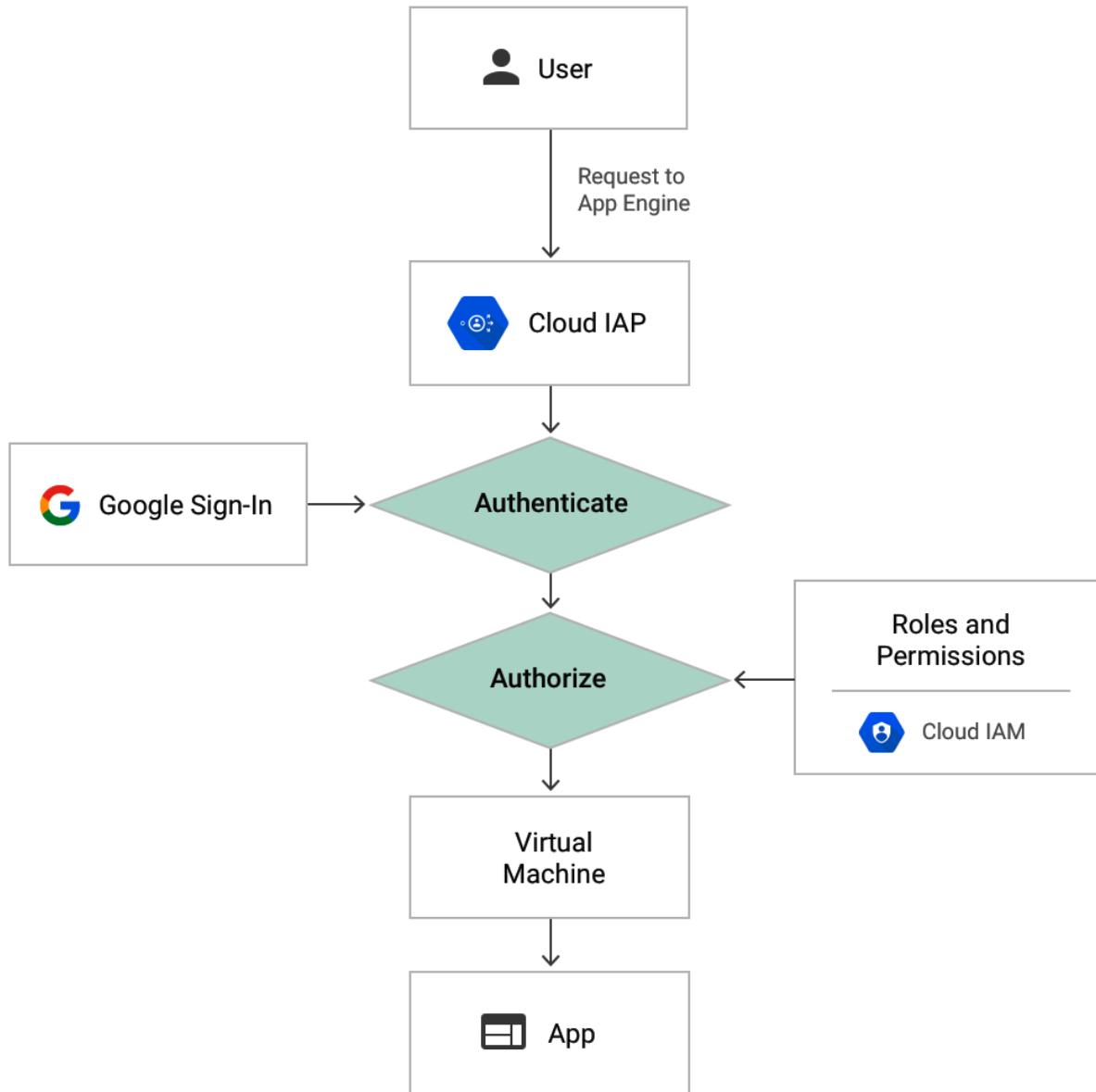


Figure 8.7 – How IAP works with App Engine

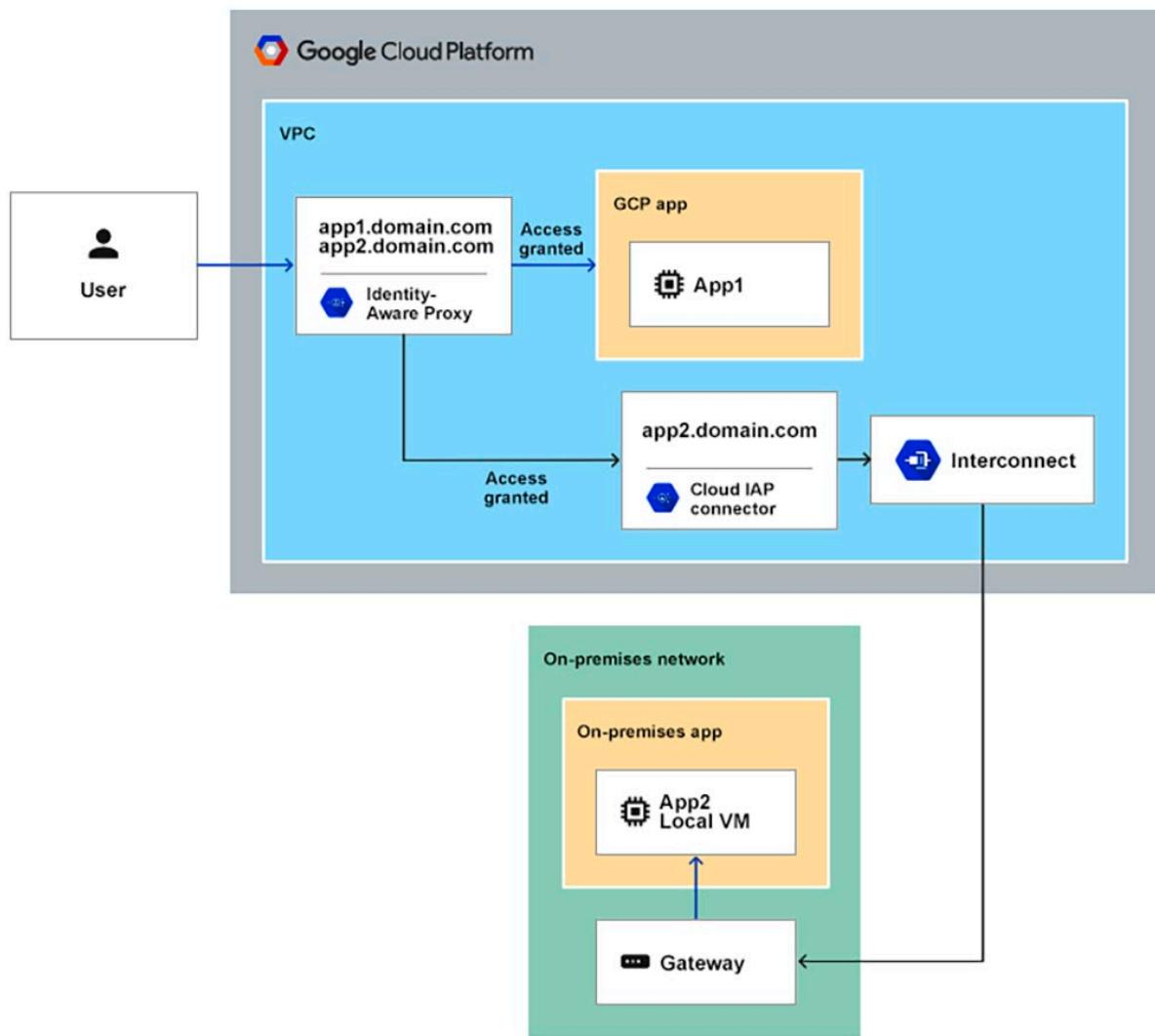


Figure 8.8 – How IAP for on-premises works

Identity-Aware Proxy (IAP) lets you manage who has access to services hosted on App Engine, Compute Engine, or an HTTPS Load Balancer. [Learn more](#)

To get started with IAP, add an [App Engine app](#), a [Compute Engine instance](#) or configure an [HTTPS Load Balancer](#).

HTTPS RESOURCES SSH AND TCP RESOURCES

Filter Enter property name or value

<input type="checkbox"/> Resource	Configuration
<input type="checkbox"/> ▼ All Tunnel Resources	
<input type="checkbox"/> ▼ us-central1-a	
<input type="checkbox"/> instance-1	Error

Figure 8.9 – The Identity-Aware Proxy dashboard

Configuration

Instance instance-1

Your firewall configuration needs to make sure that IAP can successfully connect to the individual VM. [Learn more](#)

Not enough access to resources

Cloud IAP requires a firewall that allows traffic from Cloud IAP to your VM. Add the following firewall rule to correct this issue.

Source IP range	35.235.240.0/20
Allowed protocols	tcp

Add the above rule to correct this issue **EDIT FIREWALL**

Figure 8.10 – Correcting a firewall configuration for IAP

[←](#) Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name * [?](#)

Lowercase letters, numbers, hyphens allowed

Description

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

On
 Off

Network * [▼](#) [?](#)

Priority * [CHECK PRIORITY OF OTHER FIREWALL RULES](#) [?](#)

Priority can be 0 - 65535

Direction of traffic [?](#)
 Ingress
 Egress

Action on match [?](#)
 Allow
 Deny

Targets [▼](#) [?](#)

Source filter [▼](#) [?](#)

Source IPv4 ranges * [X](#) for example, 0.0.0.0/0, 192.168.2.0/24 [?](#)

Second source filter [▼](#) [?](#)

Protocols and ports [?](#)
 Allow all
 Specified protocols and ports

tcp :

Figure 8.11 – Creating a firewall rule to enable IAP access

Identity-Aware Proxy (IAP) lets you manage who has access to services hosted on App Engine, Compute Engine, or an HTTPS Load Balancer. [Learn more](#)

To get started with IAP, add an [App Engine app](#), a [Compute Engine instance](#) or configure an [HTTPS Load Balancer](#).

HTTPS RESOURCES SSH AND TCP RESOURCES

Filter Enter property name or value

<input type="checkbox"/> Resource	Configuration ?
<input type="checkbox"/> All Tunnel Resources	
<input type="checkbox"/> us-central1-a	
<input type="checkbox"/> instance-1	<input checked="" type="checkbox"/> OK

Figure 8.12 – SSH and TCP resources after creating the firewall rule successfully

Add principals to "instance-1"

Add principals and roles for "instance-1" resource

Enter one or more principals below. Then select a role for these principals to grant them access to your resources. Multiple roles allowed. [Learn more](#)

New principals

[X](#) [?](#)

Role * [?](#)

Condition [Add condition](#) [Delete](#)

Access Tunnel resources which use Identity-Aware Proxy

+ ADD ANOTHER ROLE

SAVE **CANCEL**

Figure 8.13 – Adding a principal and applying the IAP-secured Tunnel User role

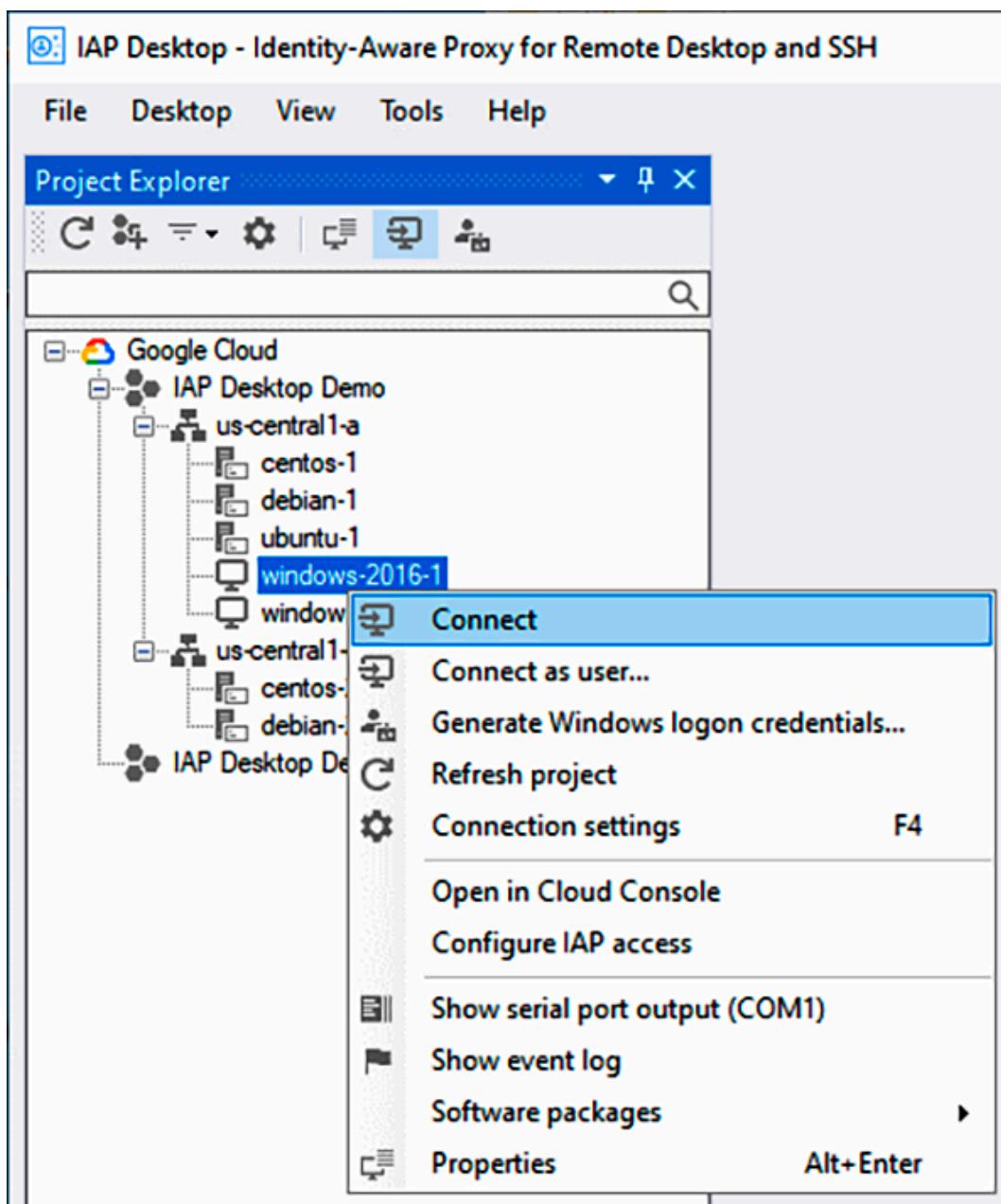


Figure 8.14 – Configuring IAP Desktop for IAP

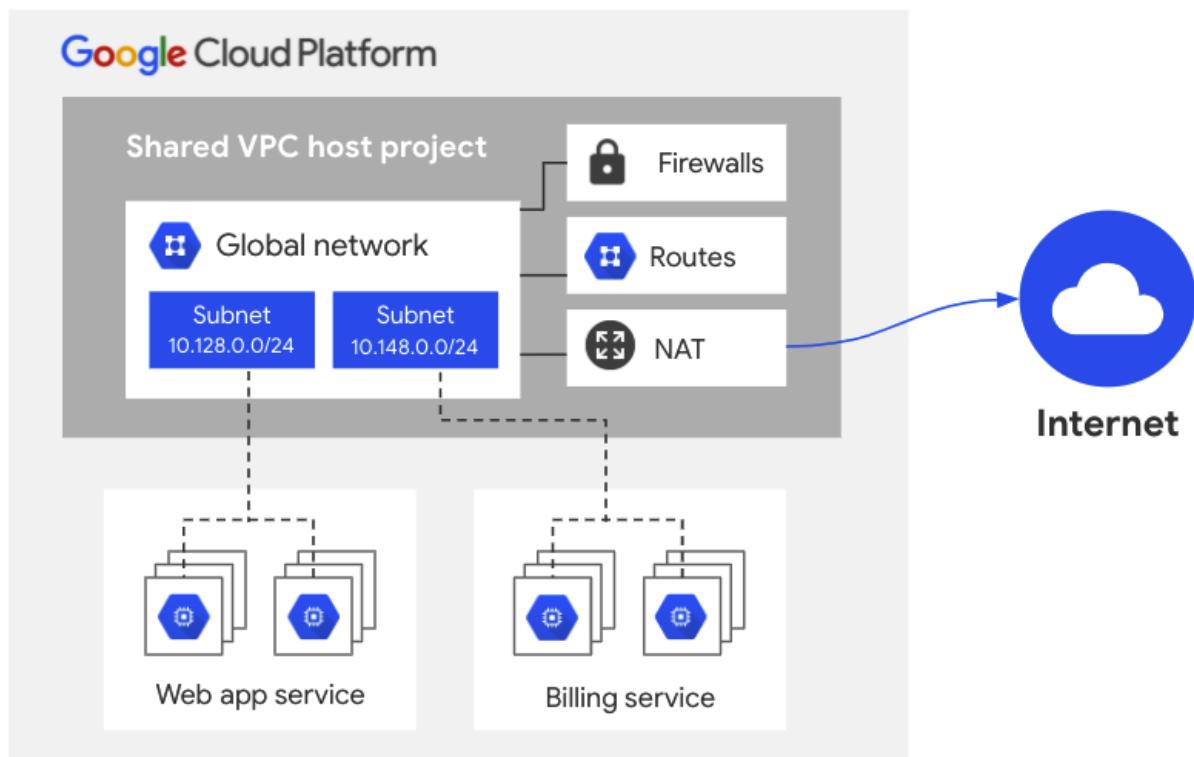


Figure 8.15 – Cloud NAT allowing outbound connections only to the internet

Network services

Cloud NAT

Cloud NAT lets your Compute Engine instances and Kubernetes Engine container pods communicate with the internet using a shared, public IP address. Cloud NAT uses a Cloud NAT gateway to connect your subnets to a Cloud Router, a virtual router that connects to the internet.

Click "Get started" to configure a Cloud NAT gateway. [Learn more](#)

GET STARTED

Figure 8.16 – Getting started with Cloud NAT

 [← Create Cloud NAT gateway](#)

 Cloud NAT lets your VM instances and container pods communicate with the internet using a shared, public IP address.

 Cloud NAT uses Cloud NAT gateway to manage those connections. Cloud NAT gateway is region and VPC network specific. If you have VM instances in multiple regions, you'll need to create a Cloud NAT gateway for each region. [Learn more](#)

 **Gateway name *** 

Lowercase letters, numbers, hyphens allowed

Select Cloud Router 

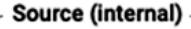
 **Network *** 

 **Region ***  

One subnet.

 **Cloud Router ***  

Cloud NAT mapping 

 **Source (internal)**  

Select which subnets to map to the Cloud NAT gateway. Primary IP addresses are used by VM instances and secondary IP addresses are used by container pods. [Learn more](#)

 **Cloud NAT IP addresses**  

Destination (external)

Internet

 **ADVANCED CONFIGURATIONS**

Figure 8.17 – Configuration to create a Cloud NAT gateway

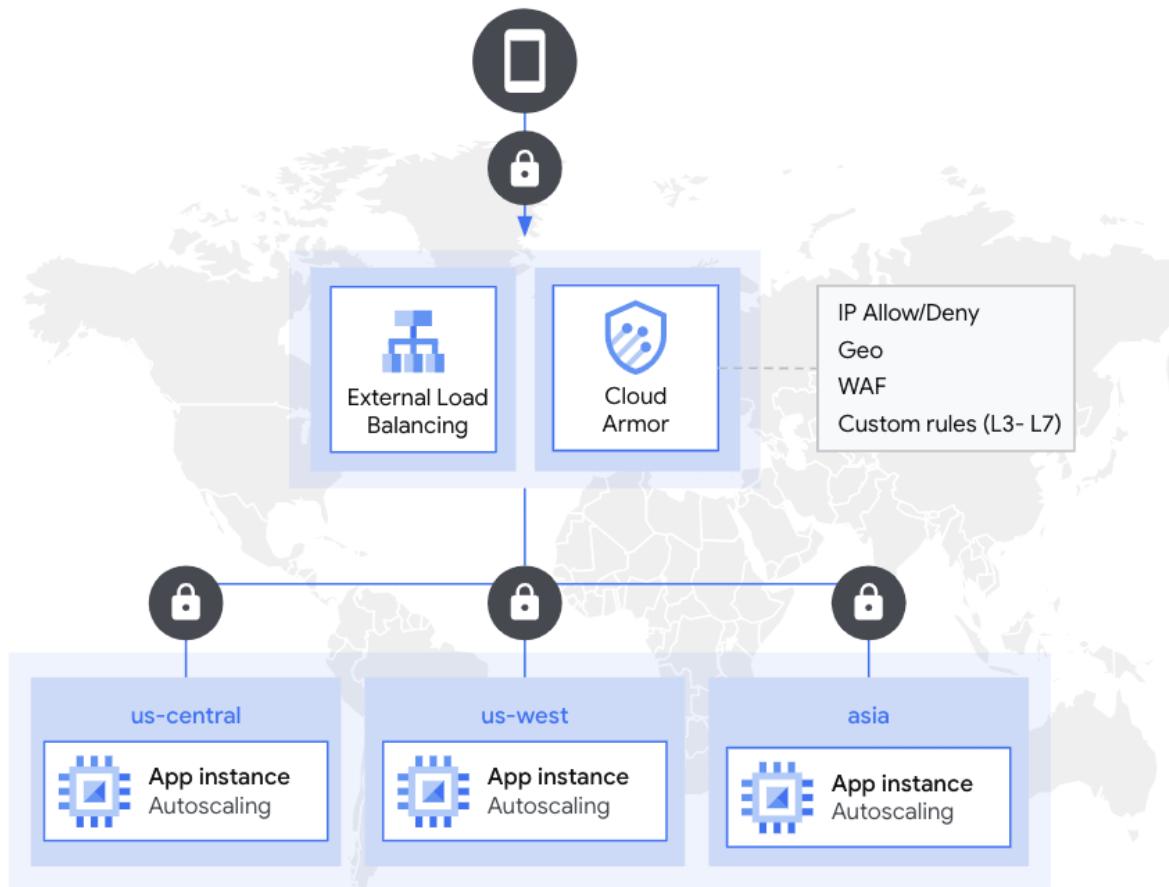


Figure 8.18 – How Google Cloud Armor secures your infrastructure

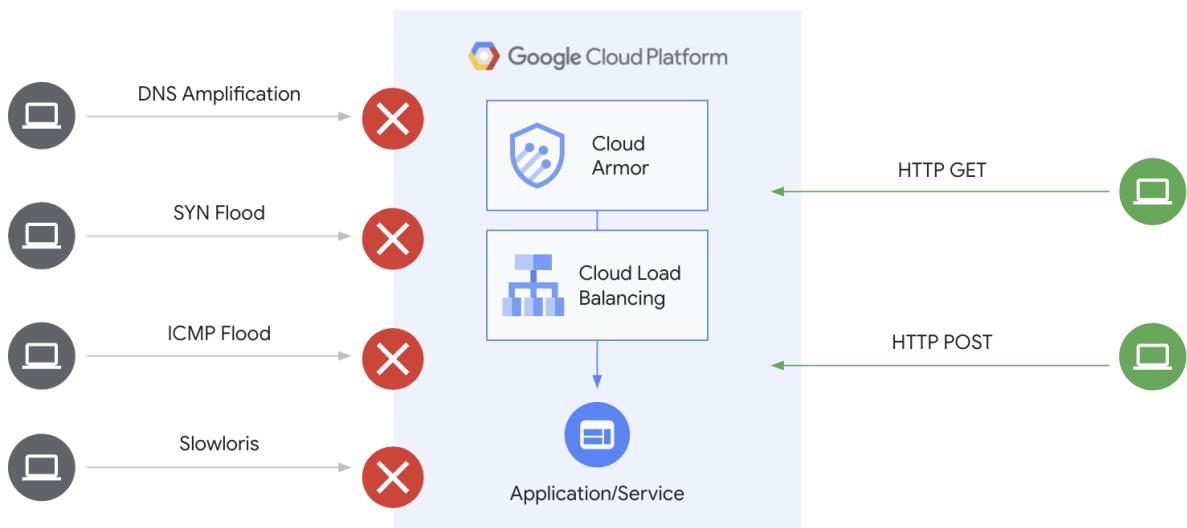


Figure 8.19 – DDoS protection against volumetric attacks

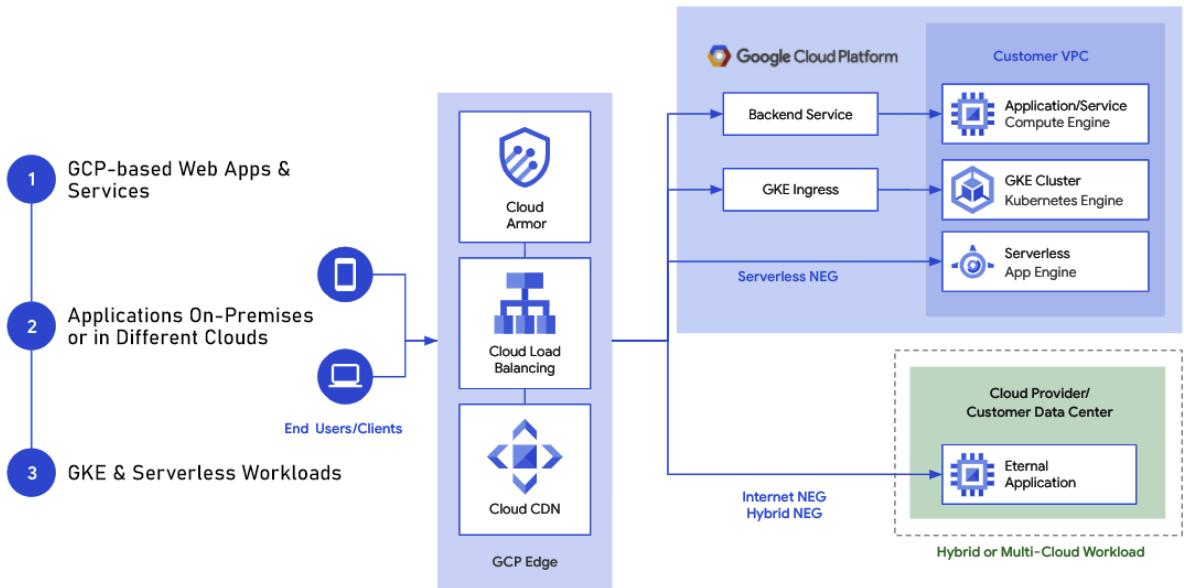


Figure 8.20 – Cloud Armor deployment models

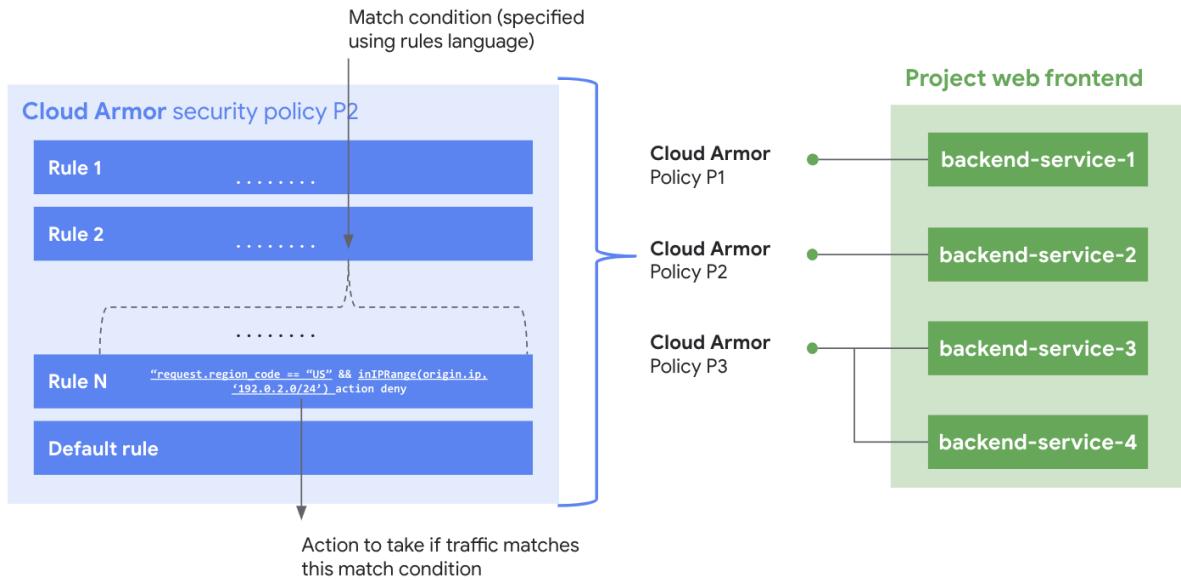


Figure 8.21 – Cloud Armor security policies

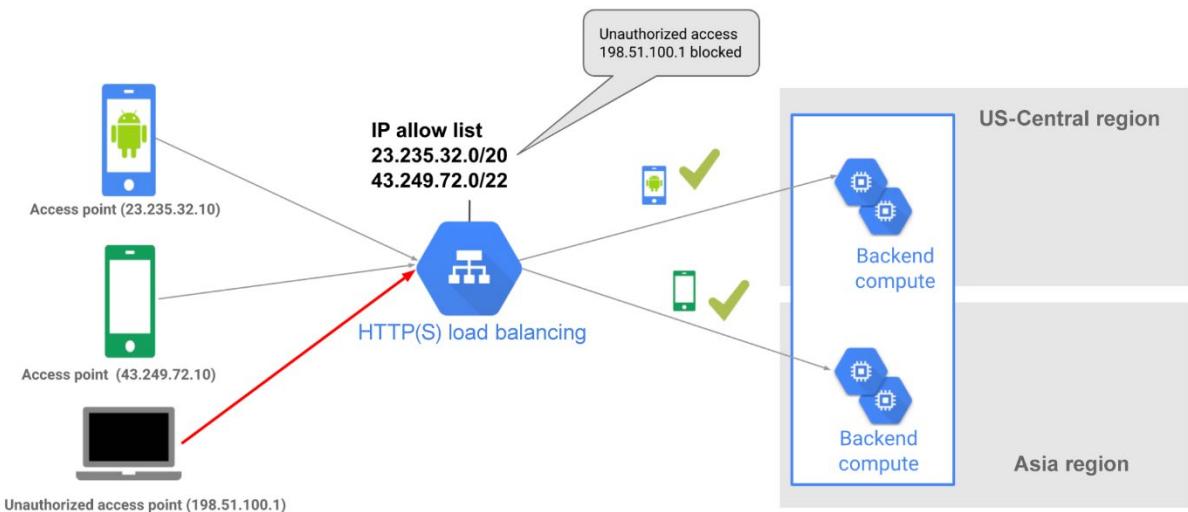


Figure 8.22 – Cloud Armor named IP list

Chapter 9: Google Cloud Key Management Service

Cloud KMS Platform

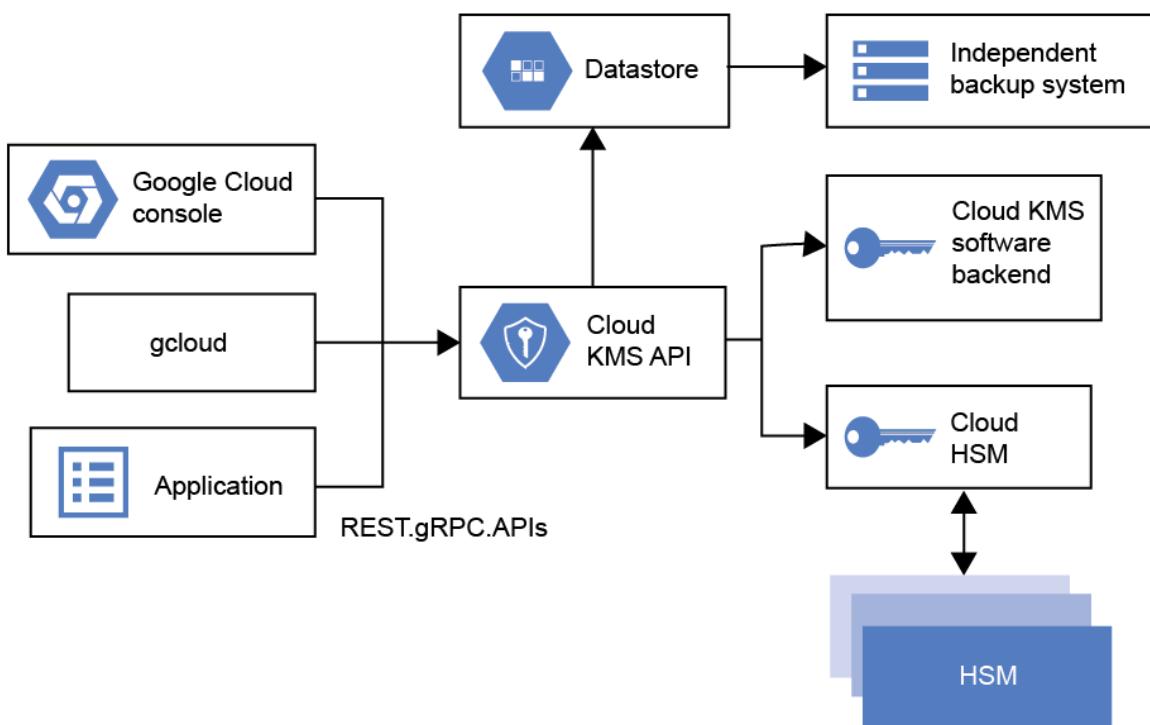


Figure 9.1 – The Cloud KMS architecture

Current Google Cloud portfolio

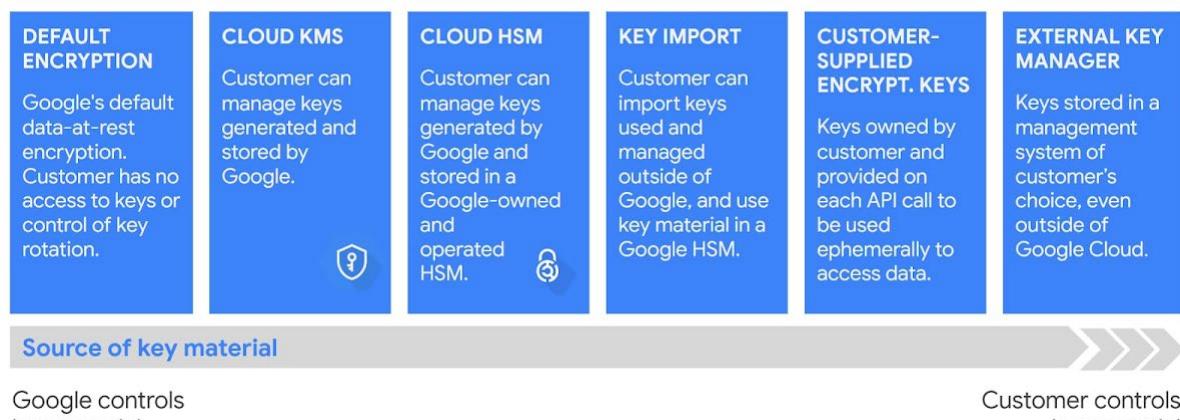


Figure 9.2 – Google Cloud encryption offerings

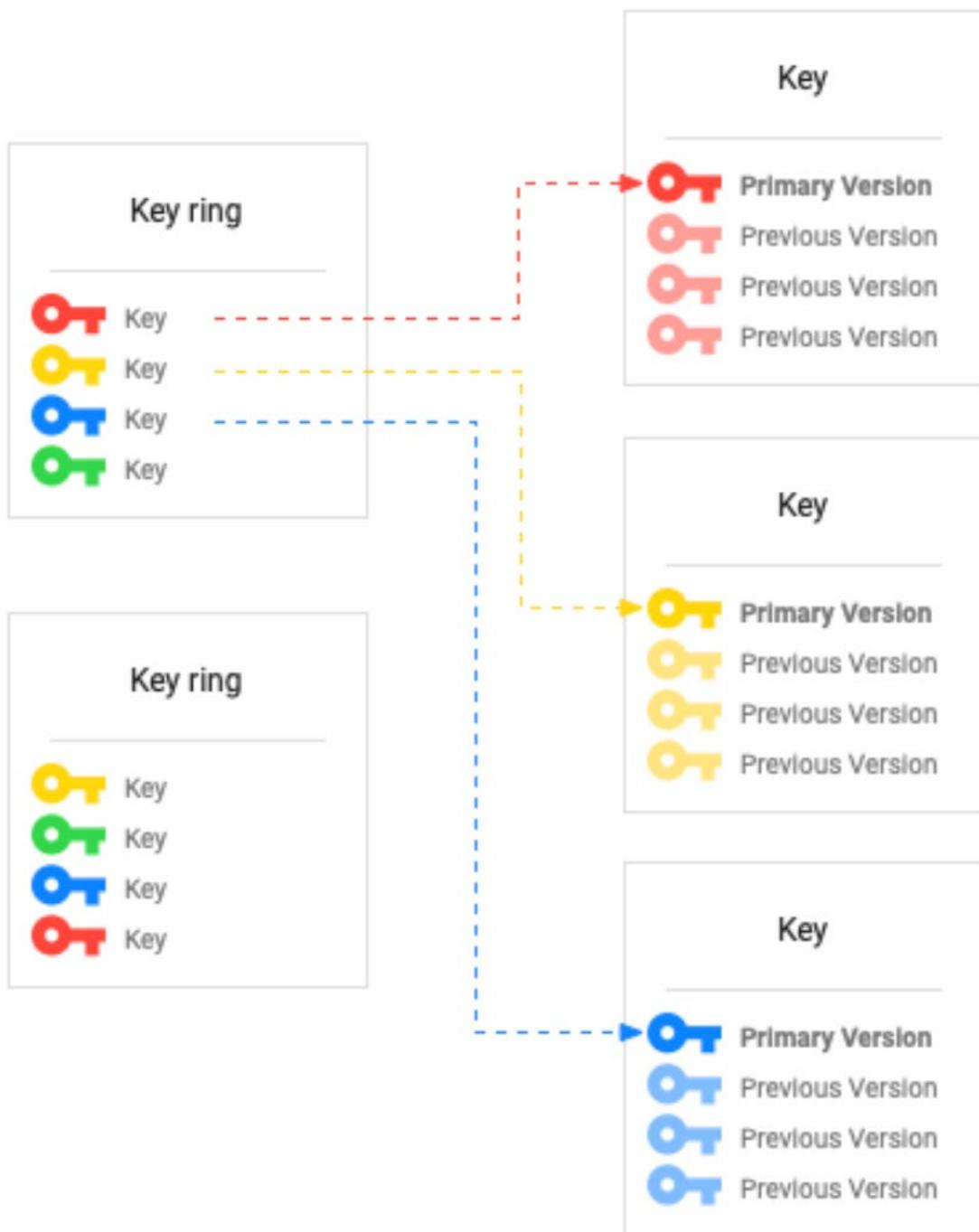


Figure 9.3 – Key structure

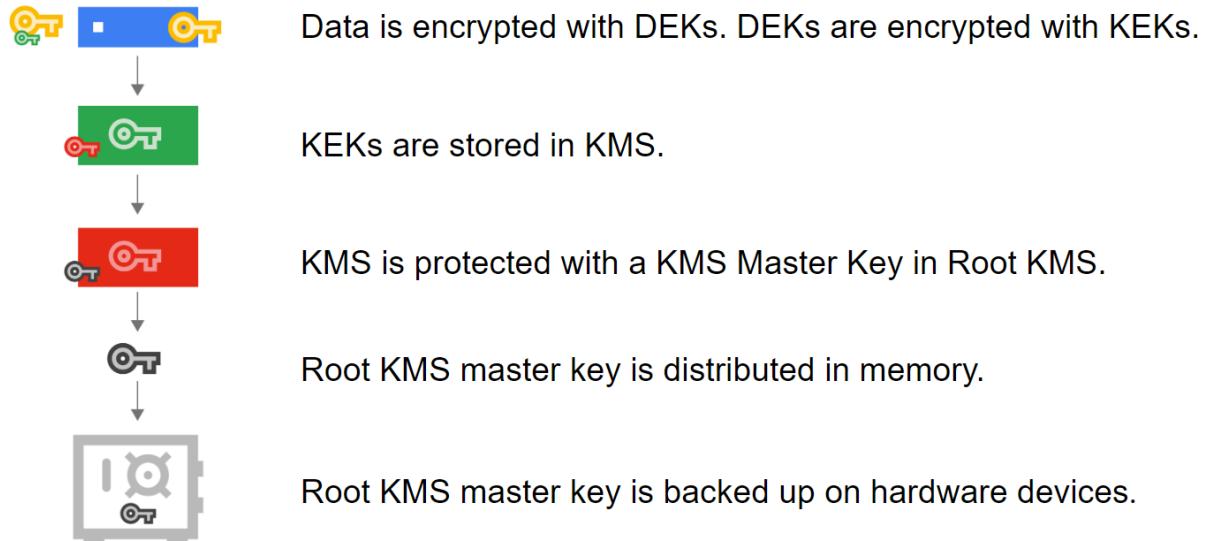


Figure 9.4 – Key hierarchy



Figure 9.5 – Envelope encryption

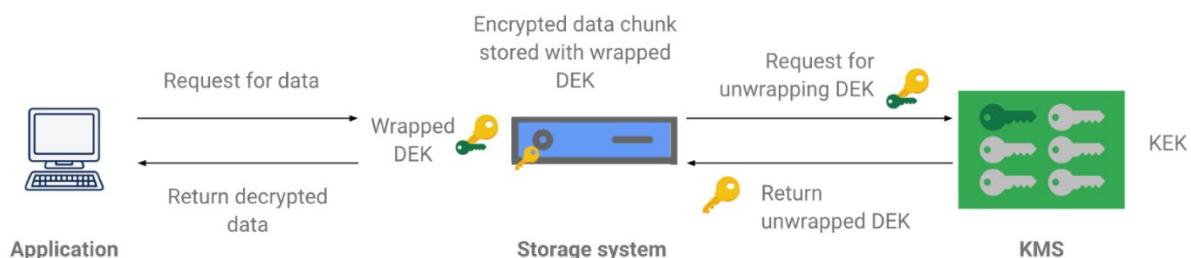


Figure 9.6 – Envelope decryption

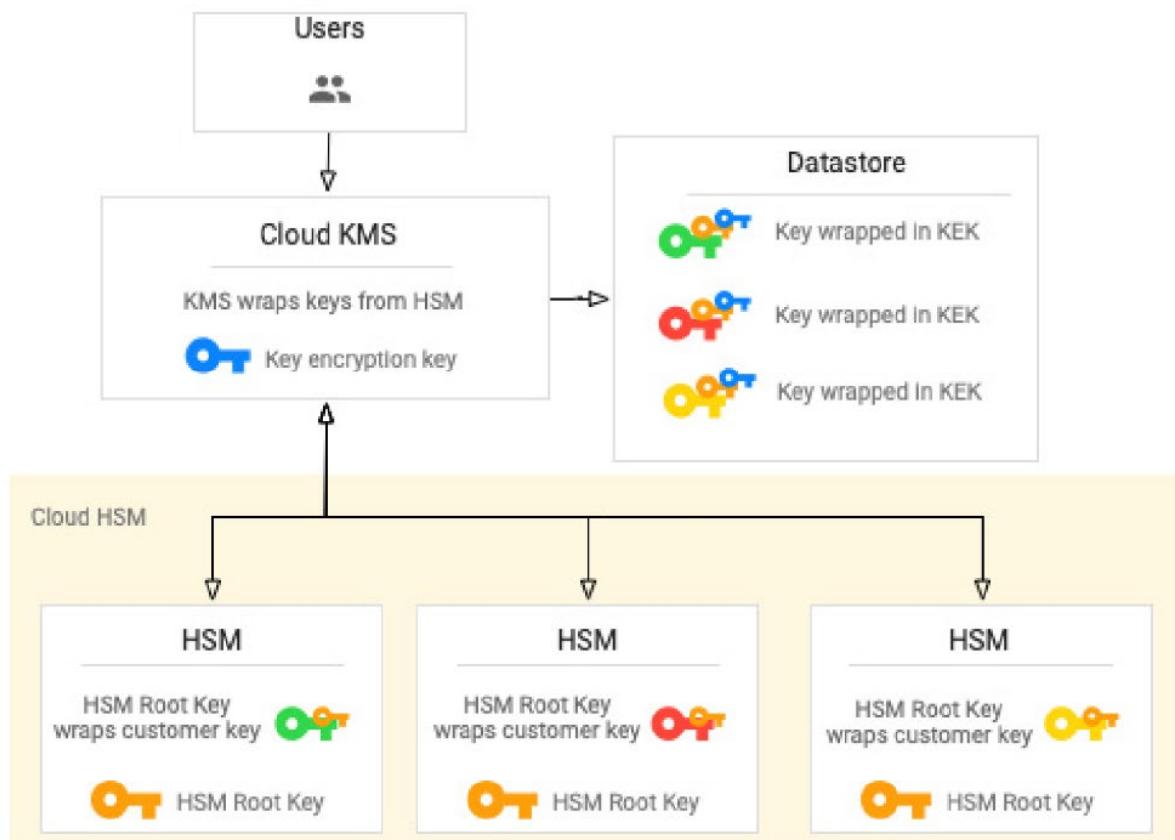


Figure 9.7 – HSM key hierarchy

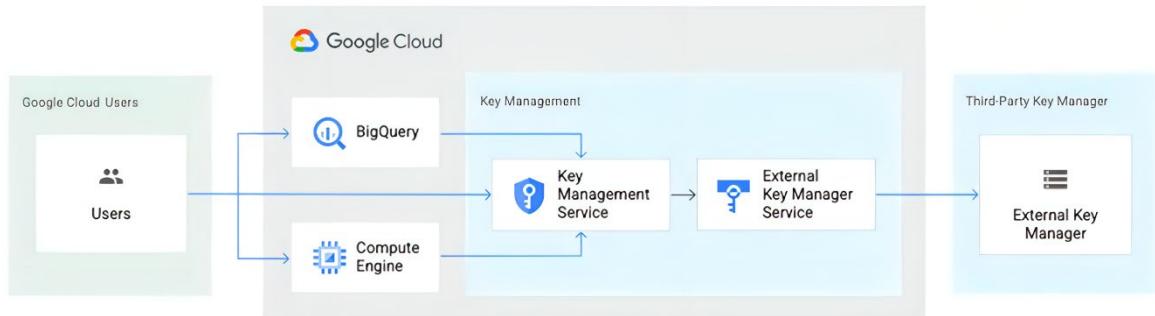


Figure 9.8 – Cloud EKM architecture

Chapter 10: Cloud Data Loss Prevention

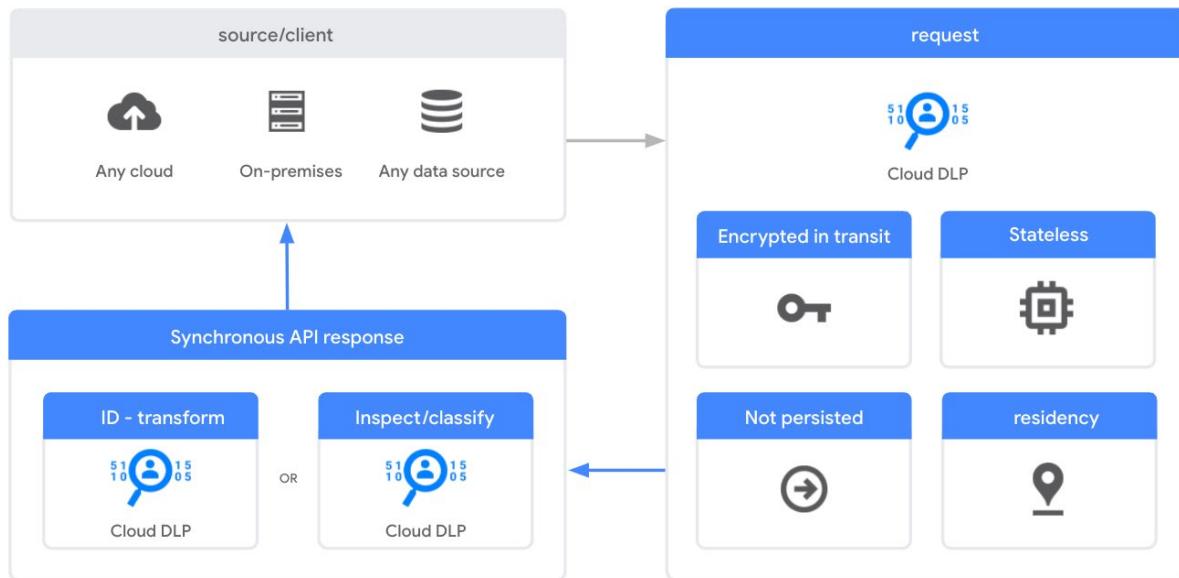


Figure 10.1 – Content method architecture

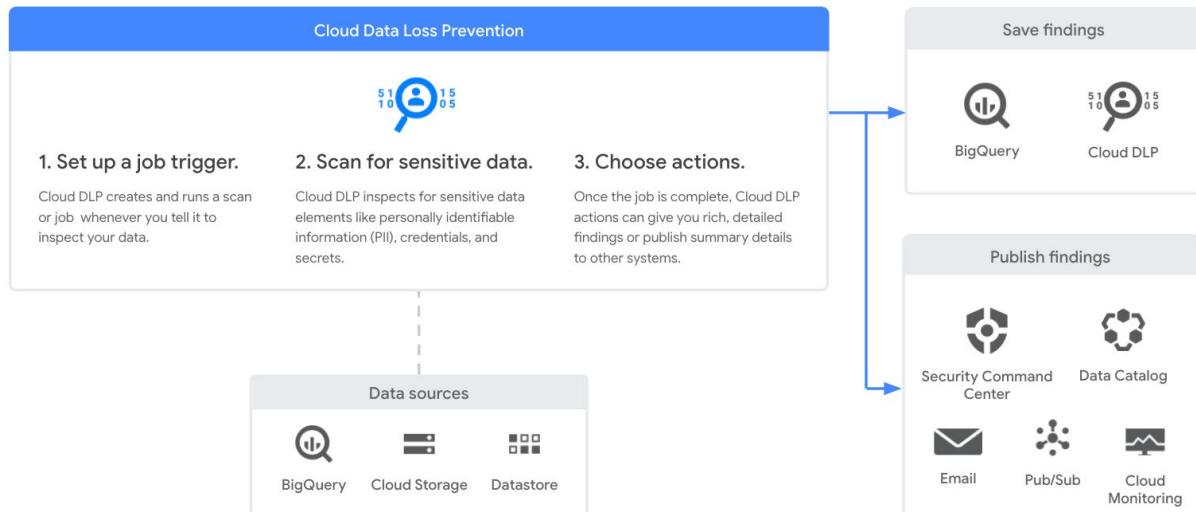


Figure 10.2 – Storage method architecture

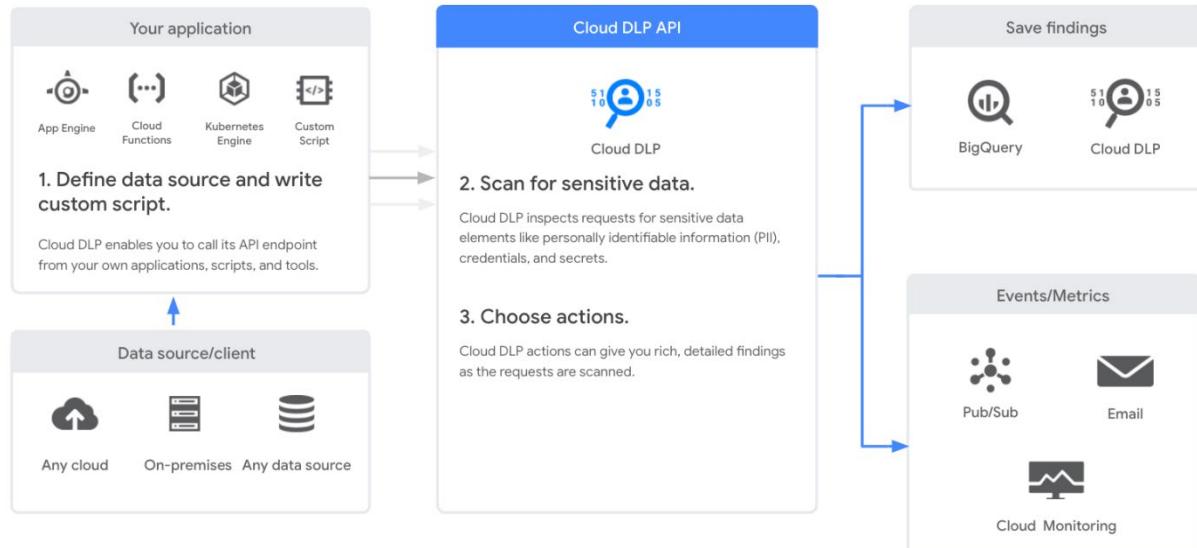


Figure 10.3 – Hybrid inspection architecture

The screenshot shows the 'Data Loss Prevention' interface. The top navigation bar includes 'CREATE', 'EXPLORE FINDINGS', 'JOBS & JOB TRIGGERS', 'CONFIGURATION' (which is selected), and 'SHOW PREVIEW PANEL'. Below this, a sub-navigation bar has 'TEMPLATES' (selected) and 'INFOTYPES' tabs, with 'INSPECT' and 'DE-IDENTIFY' buttons. A dropdown menu 'Job or job trigger' is open, showing 'Template' (which is highlighted with a red box) and 'Stored infoType'. The main content area displays a table of inspection templates:

Template ID	Display name	Resource location	Creation time	Last updated	Actions
pii-template	PII Template	Global (any region)	Jul 9, 2019, 6:07:10 PM	Jul 9, 2019, 6:07:10 PM	⋮
ssn-template	US & CAN Soc Security numbers	Global (any region)	Mar 13, 2019, 4:20:58 PM	Jun 3, 2019, 12:49:37 PM	⋮
credit-card-template	Credit cards	Global (any region)	Apr 14, 2019, 3:11:05 PM	Jun 3, 2019, 12:49:05 PM	⋮
mildly_naughty_words	Finds gently naughty words	Global (any region)	May 31, 2019, 9:57:35 AM	May 31, 2019, 9:57:35 AM	⋮

At the bottom, there are pagination controls: 'Rows per page: 30 ▾', '1 – 30 of many', and navigation arrows.

Figure 10.4 – Creating a DLP inspection template

Inspection rulesets

Adds hotword and exclusion rules to further extend built-in and custom infoType detectors with powerful context rules. [Learn more](#)

New ruleset

Choose infoTypes *

- MY_CUSTOM_INFOTYPE
- CANADA_BC_PHN

CANCEL **DONE**

ADD A RULESET

Figure 10.5 – Choosing infoTypes for Inspection rulesets

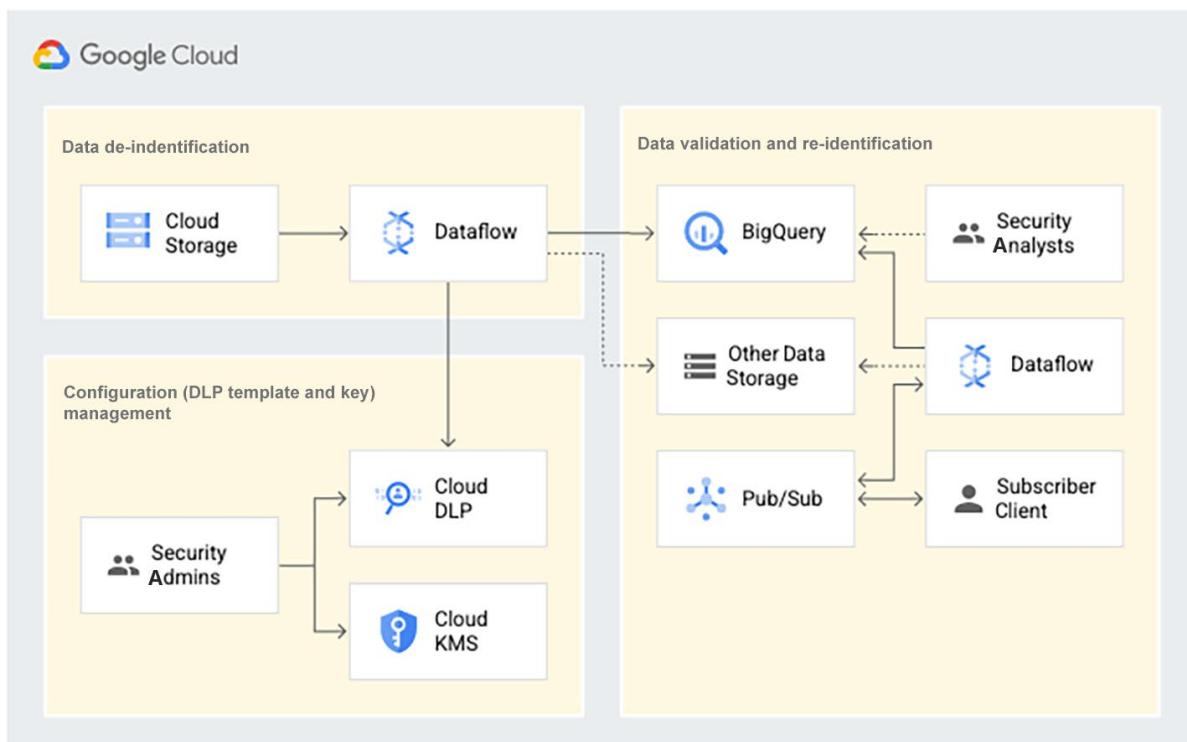


Figure 10.6 – DLP pattern for Dataflow and Data Fusion pipeline

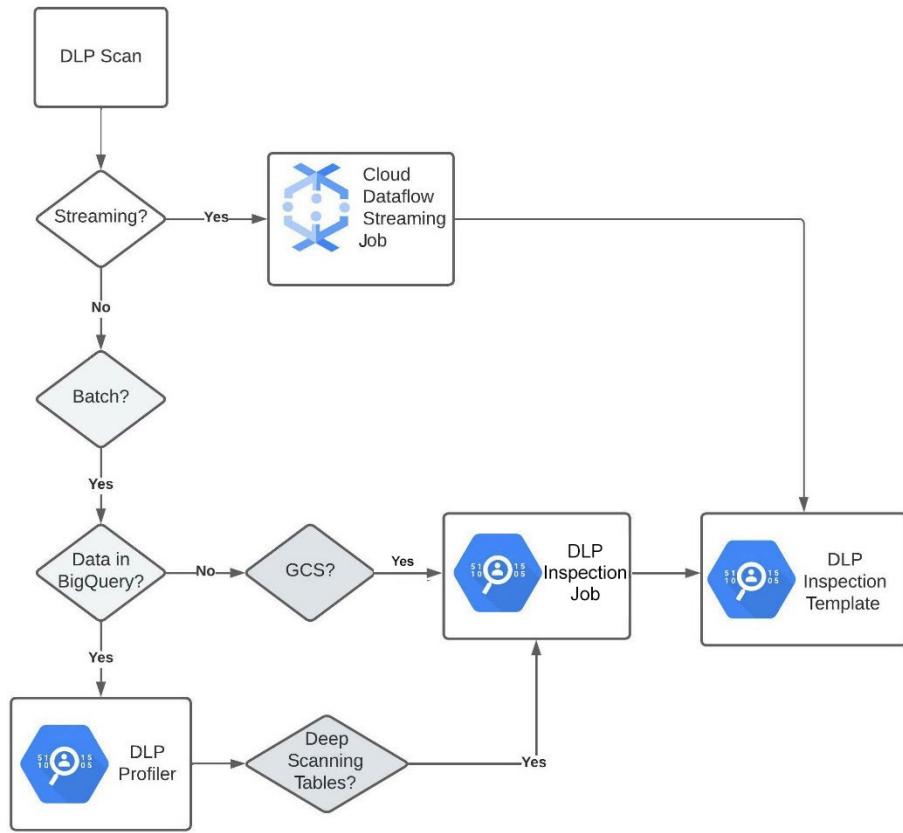


Figure 10.7 – Decision tree for inspection

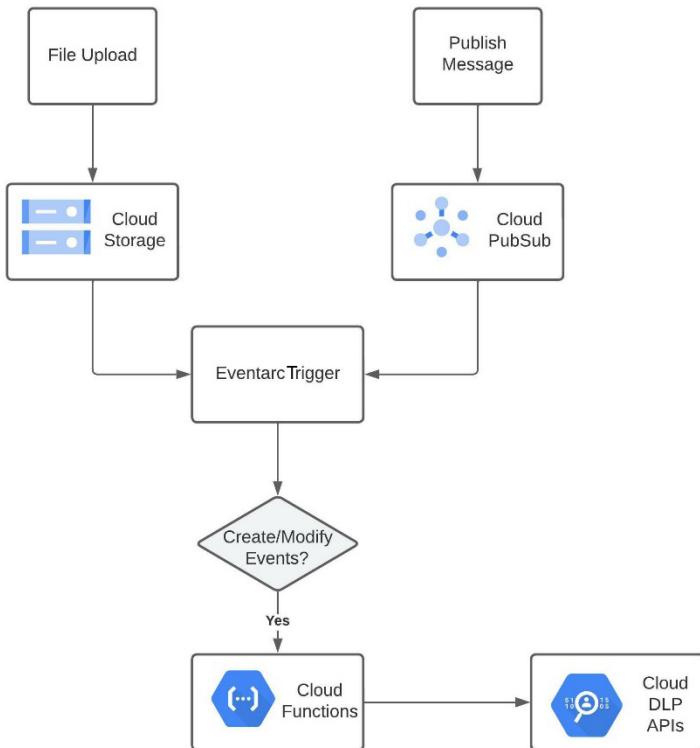


Figure 10.8 – Pattern for new updates

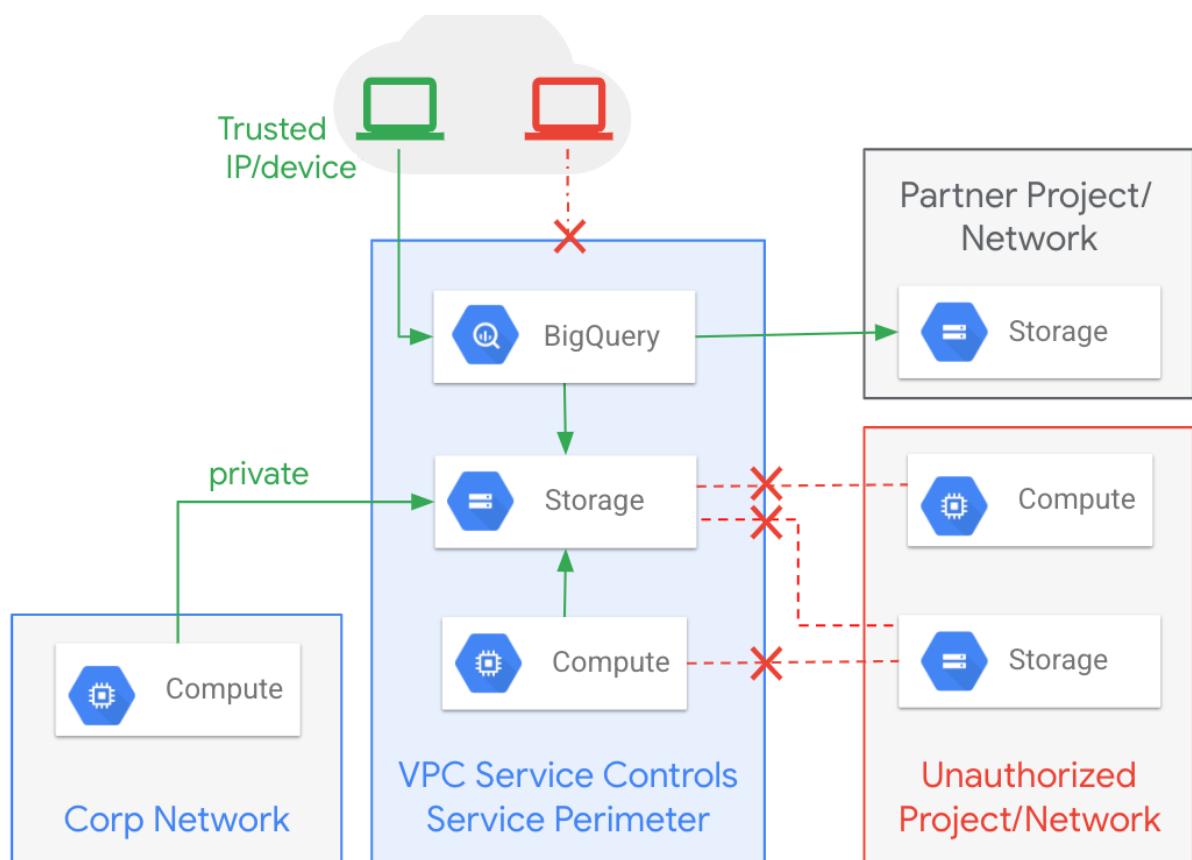


Figure 10.9 – VPC Service Controls architecture

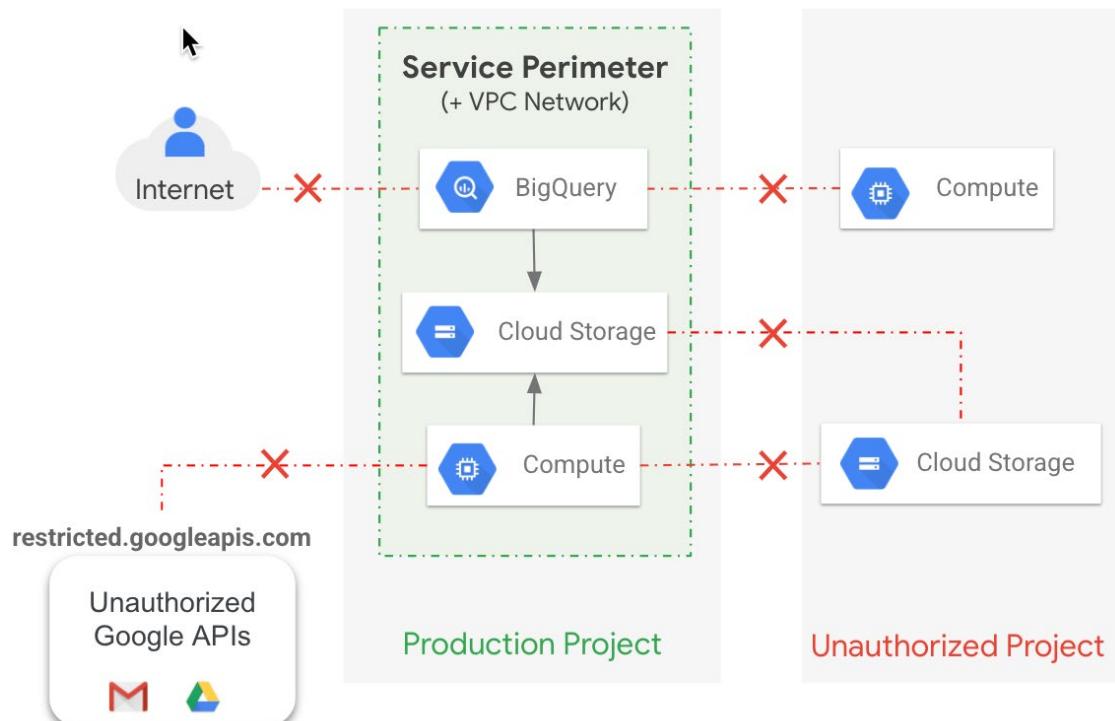


Figure 10.10 – Control APIs

New Access Level

Access level title * _____

IP_Access_Level

Access level name ?

An access level name will automatically be generated based on the title.

Create conditions in

Only conditions in the selected mode will be saved.

Basic mode ?

Advanced mode ? Premium

Conditions

Combine conditions with

OR AND

When condition is met, return:

TRUE FALSE

IP Subnetworks _____

93.184.216.0/32 ×



Enter one or more IPv4 or IPv6 subnetworks. Use CIDR block notation.

+ Geographic locations

+ Device policy Premium

SAVE

CANCEL

Figure 10.11 – Creating access level

[VPC Service Control Enforced Config Detail](#)

EDIT PERIMETER

DELETE PERIMETER

Basic details

Perimeter Title

sp_higher_trust_analytics_yzxm

Perimeter Name

accessPolicies/626444471578/servicePerimeters/sp_higher_trust_analytics_yzxm

Perimeter Type

Regular

Projects to protect

No projects

Restricted Services

BigQuery API

Google Cloud Asset API

Google Cloud Data Catalog API

Google Cloud Dataflow API

Google Cloud Data Loss Prevention (DLP) API

Cloud Functions API

Cloud Key Management Service (KMS) API

Stackdriver Logging API

Google Cloud Pub/Sub API

Secret Manager API

Google Cloud Storage API

Google Compute Engine API

Cloud Monitoring API

AI Platform Notebooks API

VPC Accessible Services

All services allowed

Access Levels

alp_higher_trust_analytic_yzxm

Ingress policy

No ingress policy

Egress policy

Figure 10.12 – Defining a service perimeter

Chapter 11: Secret Manager

[←](#) Create secret

Secret details

This will create a secret with the secret value in the first version. [Learn more](#)

Name *

 Secret name is required

Secret value

Input your secret value or import it directly from a file.

Upload file

BROWSE

Maximum size: 64 KiB

Secret value

Replication policy

By default, Google automatically manages where this secret is stored. If you need to manually manage this, you can customize the locations by checking the box below. All secrets are globally accessible regardless of how they are replicated and stored. The replication policy cannot be changed after a secret is created. [Learn more](#)

Manually manage locations for this secret

Encryption

This secret is encrypted with a Google-managed key by default. If you need to manage your encryption, you can use a customer-managed key instead. [Learn more](#)

Use a customer-managed encryption key (CMEK)

Figure 11.1 – Creating a new secret

Rotation

Setting a rotation period will send rotation notifications to Pub/Sub topics. Secret Manager will not automatically rotate the secret value. [Learn more](#)

Set rotation period

Notifications

Select Pub/Sub topic(s) that will receive event notifications whenever the secret or one of its versions is changed. These events can be user initiated changes or scheduled events. [Learn more](#)

[+ ADD TOPIC](#)

Expiration

By default, the secret never expires. To set an expiration date for this secret, select Set expiration date below. If you choose an expiration date, the secret will be deleted and unavailable after that time. [Learn more](#)

Set expiration date

Labels

Use labels to organize and categorize your secrets.

[+ ADD LABEL](#)

Figure 11.2 – Creating a new secret—rotation period

Secret: "apiKey"

projects/794301636481/secrets/apiKey

OVERVIEW	VERSIONS	PERMISSIONS	LOGS
Versions	+ NEW VERSION	ENABLE	DISABLE
		Created on 	Actions
<input checked="" type="checkbox"/>	Version	Status	Encryption
<input checked="" type="checkbox"/>	1	 Enabled	Google-managed
		5/16/22, 5:02 PM	

1 version selected

Figure 11.3 – Adding a new secret version

Add new version to "apiKey"

Input the new secret value or import it directly from a file.

Upload file [BROWSE](#)

Maximum size: 64 KiB

Secret value

Disable all past versions

[CANCEL](#) [ADD NEW VERSION](#)

Figure 11.4 – Adding a new secret version (continued)

Secret: "apiKey"

projects/794301636481/secrets/apiKey

OVERVIEW	VERSIONS	PERMISSIONS	LOGS	
Versions	+ NEW VERSION	ENABLE	DISABLE	DESTROY
✓	Version	Status	Encryption	Created on ↓ Actions
	1	⚠ Disabled	Google-managed	5/16/22, 5:02 PM ⋮

1 version selected

Figure 11.5 – Disabling a secret

Secret: "apiKey"

projects/794301636481/secrets/apiKey

OVERVIEW	VERSIONS	PERMISSIONS	LOGS	
Versions	+ NEW VERSION	ENABLE	DISABLE	DESTROY
	Version	Status	Encryption	Created on ↓
	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> Enabled	Google-managed	5/16/22, 5:02 PM

1 version selected

Figure 11.6 – Enabling a secret

Chapter 12: Cloud Logging

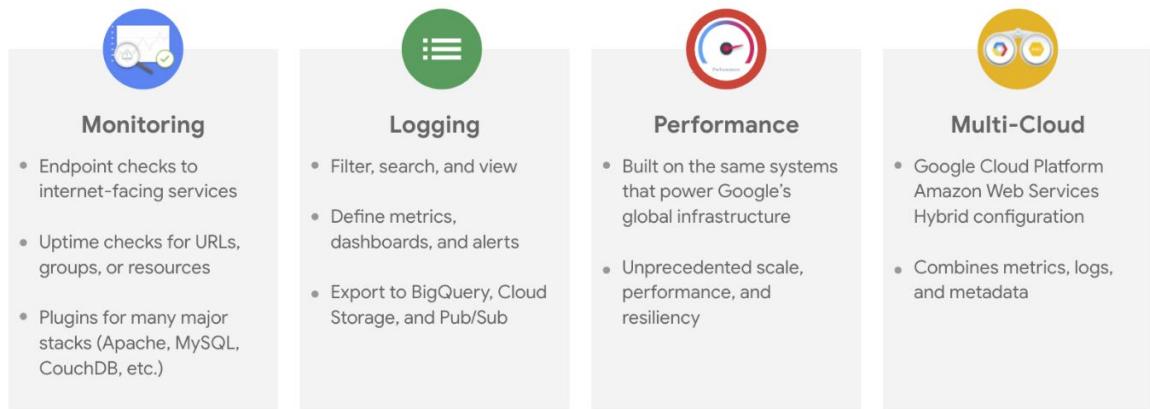


Figure 12.1 – Google Cloud’s operations suite

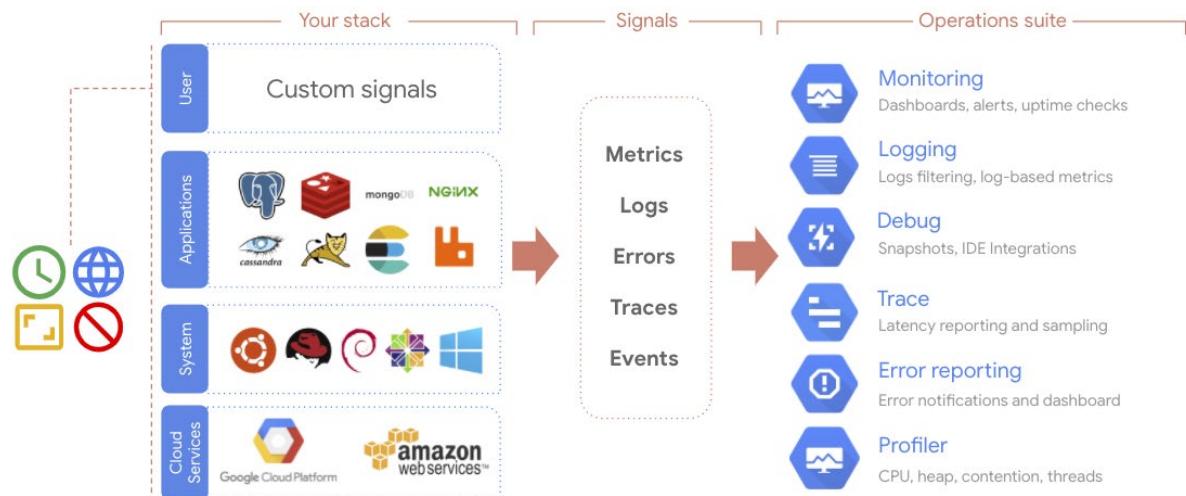


Figure 12.2 – Operations suite layers



Figure 12.3 – Log categories

	Retention	Cost
 Admin Activity audit logs	13 months (400 days)	Free
System Event audit logs	13 months (400 days)	Free
Access Transparency logs	13 months (400 days)	Free
Data Access audit logs	30 days	\$0.50 per GB over 50GB/Month
All other logs	30 days	\$0.50 per GB over 50GB/Month
Workspace admin console logs	6 months	Free
Log sink	Indefinite	Based on service option (GCS, BQ, Pub/Sub)

Figure 12.4 – Cloud Logging default retention periods and costs

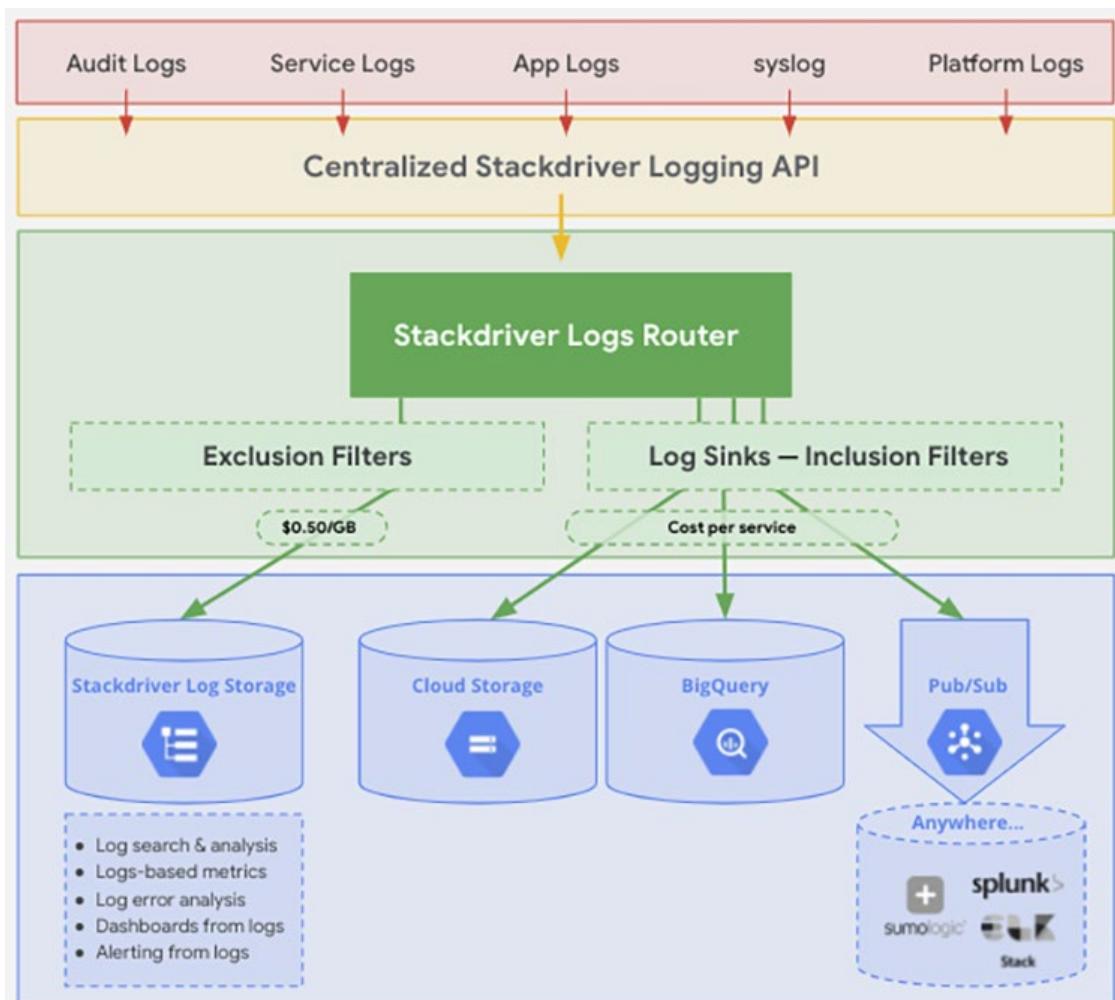


Figure 12.5 – Log Router

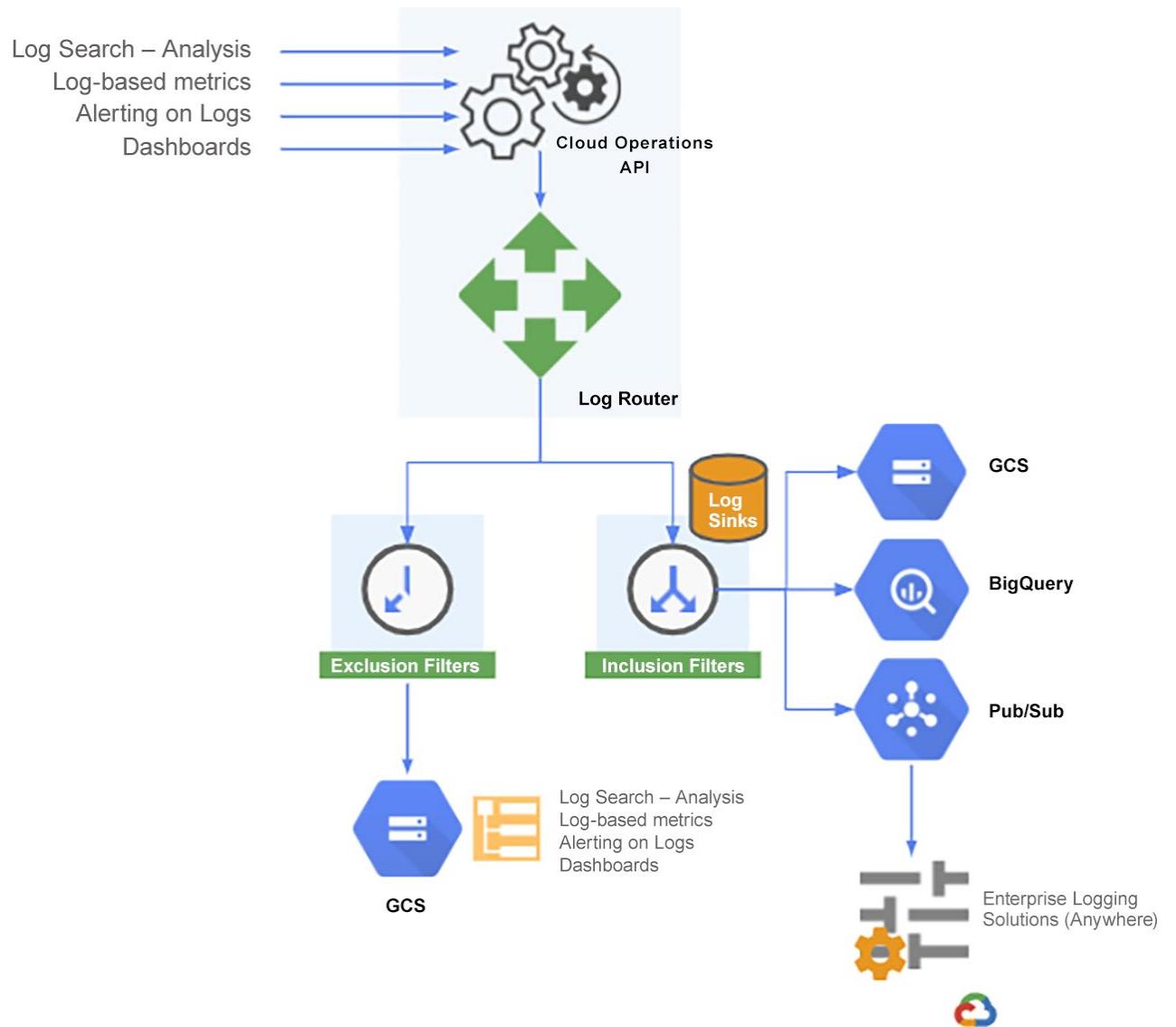


Figure 12.6 – Log exports and sinks

Google Cloud My First Project

Operations Logging Logs Explorer Logs Dashboard Log-based Metrics Log Router Log Storage Log Analytics Integrations

Create log bucket

1 Bucket details

Provide a name and description for the log bucket.

Name * my-regional-bucket

Ex. 'example' or 'example_bucket-1'

Description

Upgrade to use Log Analytics
You cannot downgrade a log bucket after it has been upgraded. [Learn more](#)

Select log bucket region * australia-southeast1

Log bucket regions can't be changed later.

NEXT

2 Set the retention period

Choose the duration that logs are stored in the bucket.

CREATE BUCKET CANCEL

Figure 12.7 – Create log bucket

Create log bucket

Bucket details

Provide a name and description for the log bucket.

Name my-regional-bucket
Description
Region australia-southeast1

Set the retention period

Choose the duration that logs are stored in the bucket. Setting a longer retention period impacts billing.

Retention period * 30 day(s)

CREATE BUCKET CANCEL

Figure 12.8 – Set the retention period for the log bucket

Create logs routing sink

Sink details
 Provide a name and description for logs routing sink
Name my-log-sink
Description

Sink destination
 Select the service type and destination for logs routing sink. Logs routed to Cloud Storage are written in hourly batches while other sink types are processed in real time.
Service Destination Cloud Logging bucket
`logging.googleapis.com/projects/ [rst]`

Choose logs to include in sink
 Create an inclusion filter to determine which logs are included in logs routing sink
Inclusion filter

Choose logs to filter out of sink (optional)
 Create exclusion filters to determine which logs are excluded from logs routing sink
Build an exclusion filter **+ ADD EXCLUSION**

CREATE SINK **CANCEL**

Figure 12.9 – Create a log sink

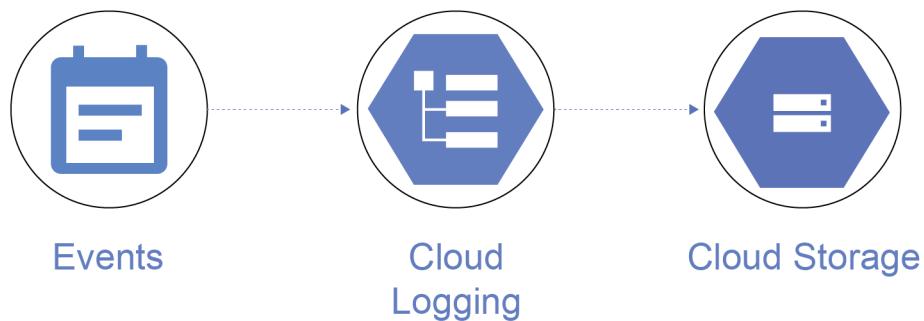


Figure 12.10 – Log archiving pipeline

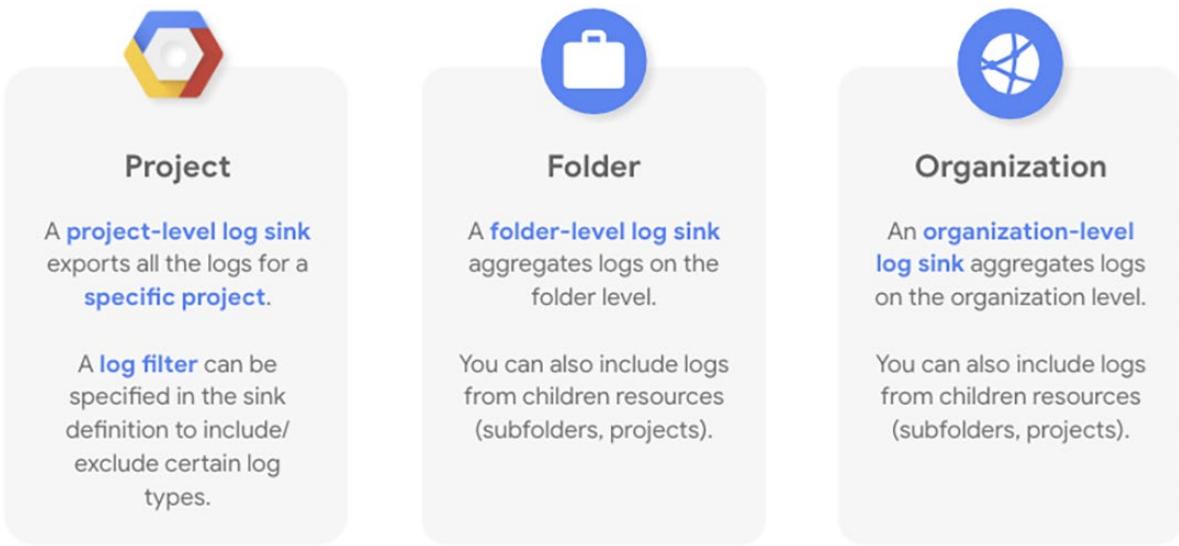


Figure 12.11 – Log aggregation



Figure 12.12 – Log streaming pipeline

☰ Google Cloud

My First Project ▾

Cloud Storage	← Create a Bucket
Buckets	Name your bucket Name: my-log-bucket-for-demo
Monitoring NEW	Choose where to store your data Location: us (multiple regions in United States) Location type: Multi-region
Settings	Choose a storage class for your data Default storage class: Standard
	Choose how to control access to objects Public access prevention: On Access control: Uniform
	Choose how to protect object data Your data is always protected with Cloud Storage but you can also choose from these additional data protection options to prevent data loss. Note that object versioning and retention policies cannot be used together. Protection tools <input type="radio"/> None <input type="radio"/> Object versioning (for data recovery) For restoring deleted or overwritten objects. To minimise the cost of storing versions, we recommend limiting the number of non-current versions per object and scheduling them to expire after a number of days. Learn more ↗ <input checked="" type="radio"/> Retention policy (for compliance) For preventing the deletion or modification of the bucket's objects for a specified minimum duration of time after being uploaded. Learn more ↗ Duration * 5 years ▾
	DATA ENCRYPTION
	CREATE CANCEL

Figure 12.13 – Create a Cloud Storage bucket for logs

The screenshot shows the Google Cloud Storage interface for a bucket named "my-log-bucket-for-demo". The "Lifecycle" tab is selected. The bucket details are as follows:

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Not public	Retention: 5 years

The Lifecycle section contains a note: "After you have added or edited a rule, it may take up to 24 hours to take effect." Below this, a list of rules is shown:

Action	Object condition	Works with
Set to Nearline	60+ days since object was created	trash edit
Set to Coldline	120+ days since object was created	trash edit

A message at the bottom states: "You haven't added any lifecycle rules to this bucket."

Figure 12.14 – The LIFECYCLE tab

This screenshot is identical to Figure 12.14, but it includes two lifecycle rules:

Action	Object condition	Works with
Set to Nearline	60+ days since object was created	trash edit
Set to Coldline	120+ days since object was created	trash edit

Figure 12.15 – Add a rule for lifecycle management

Chapter 13: Image Hardening and CI/CD Security

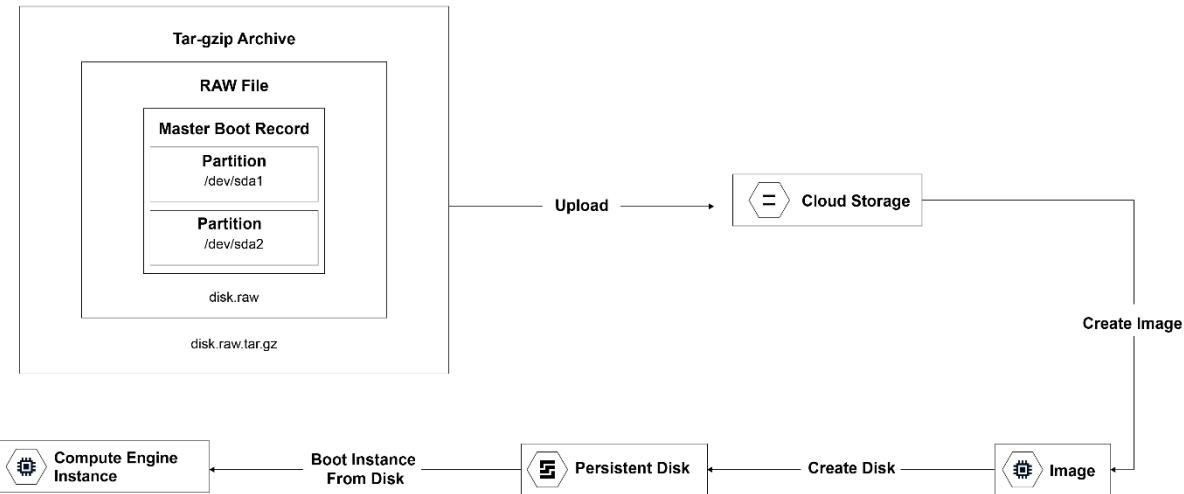


Figure 13.1 – A pipeline for creating a VM image

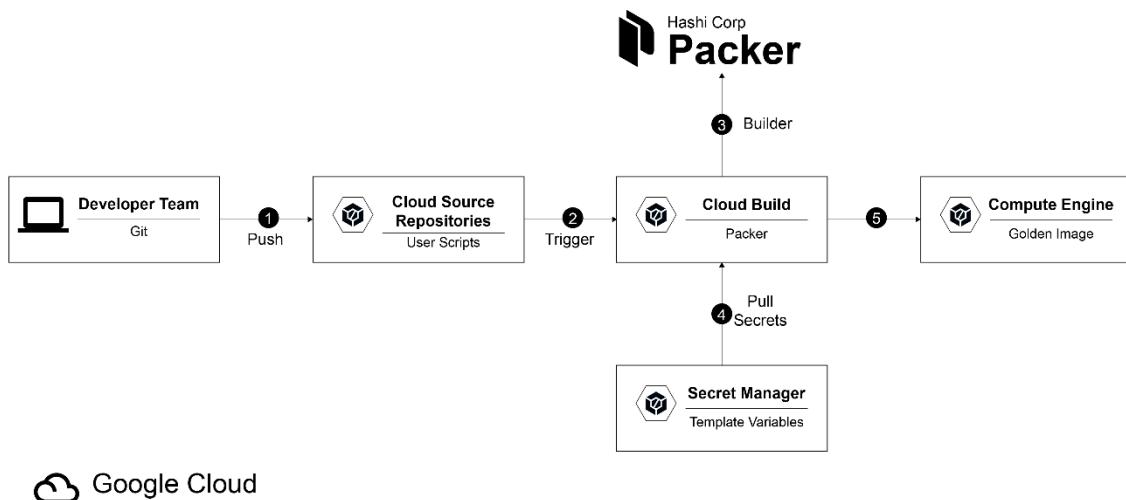


Figure 13.2 – VM image creation using Packer

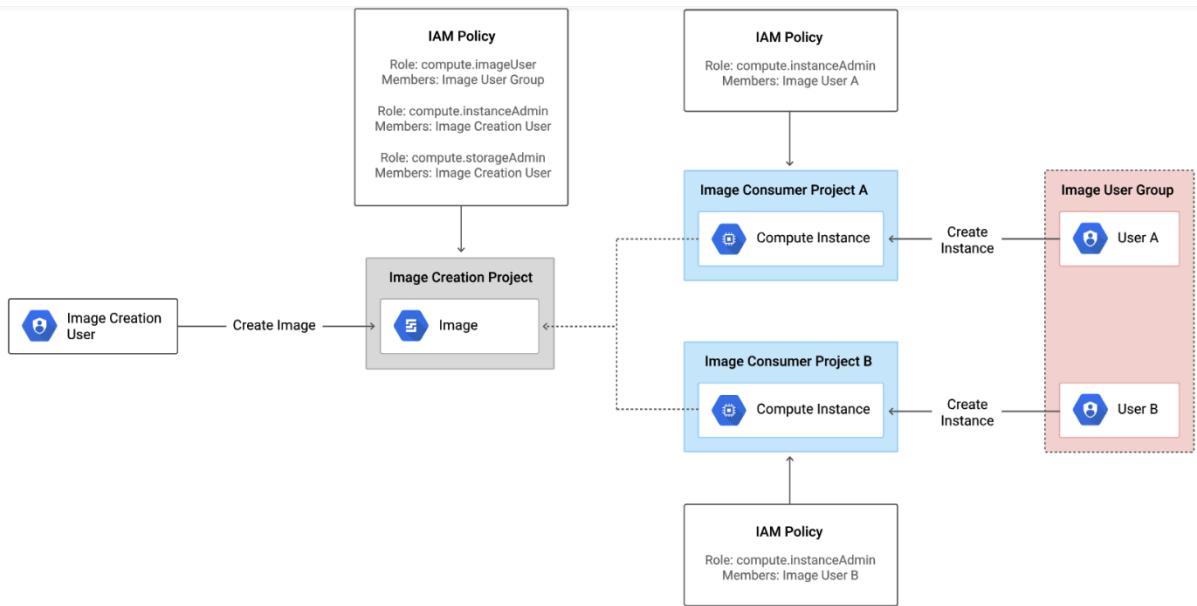


Figure 13.3 – Sharing images between projects

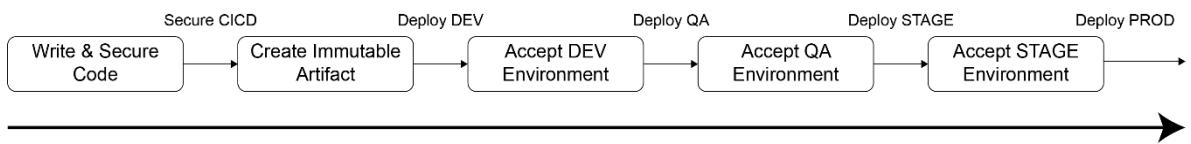


Figure 13.4 – Artifact trust

Chapter 14: Security Command Center

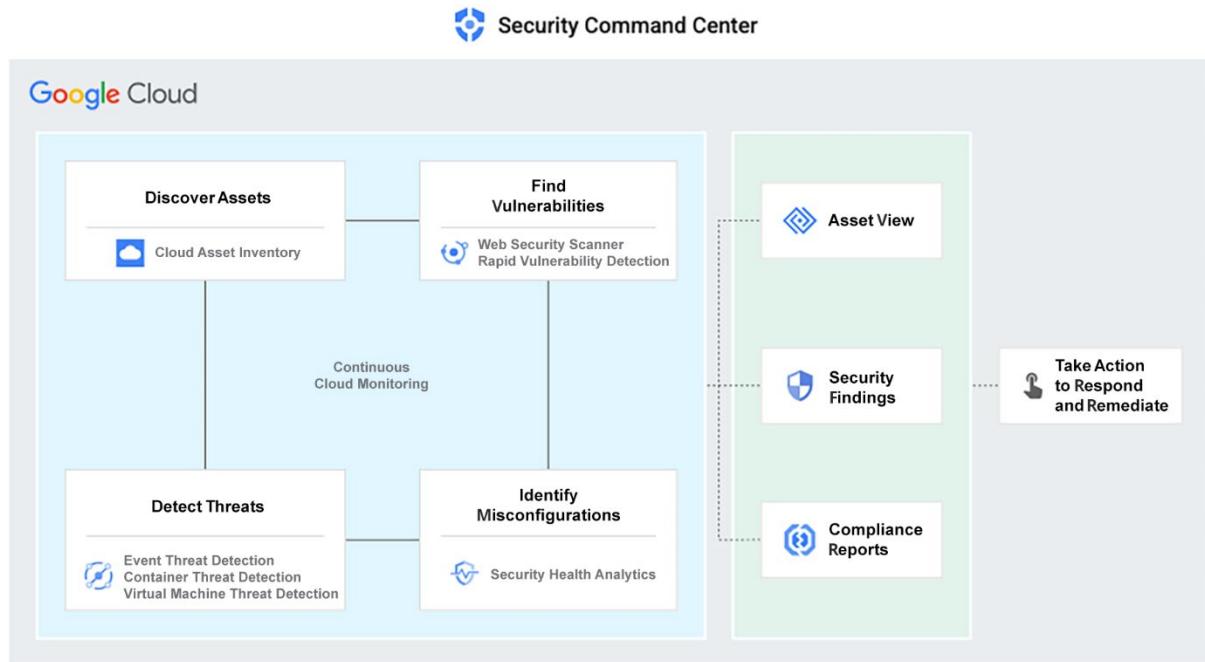


Figure 14.1 – SCC core services

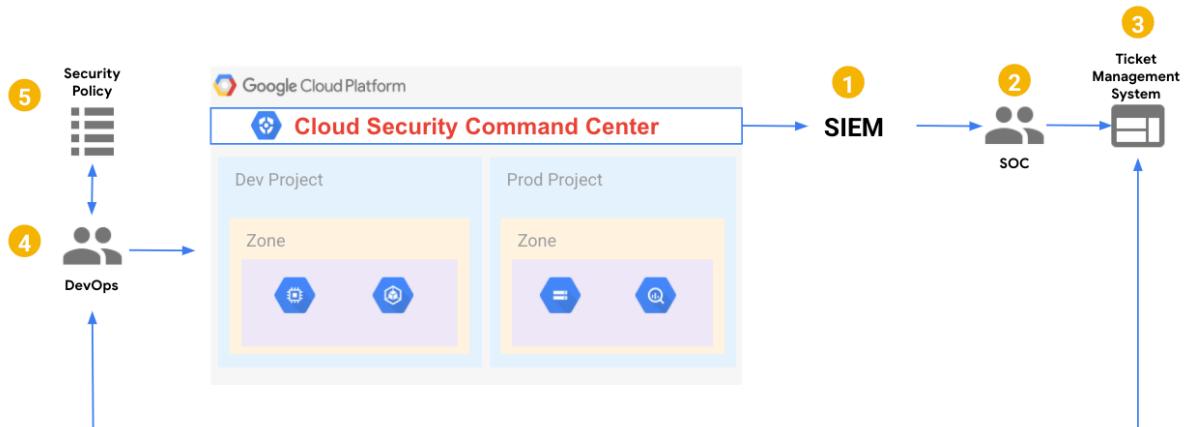


Figure 14.2 – Automating SCC response

Chapter 15: Container Security

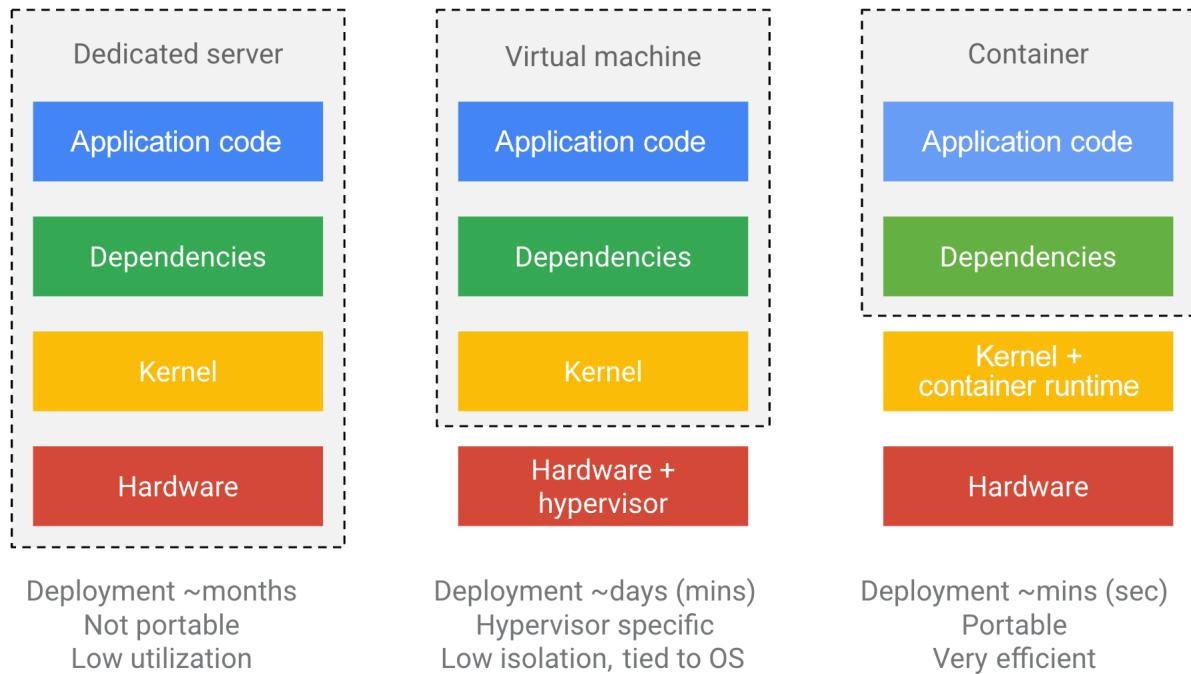
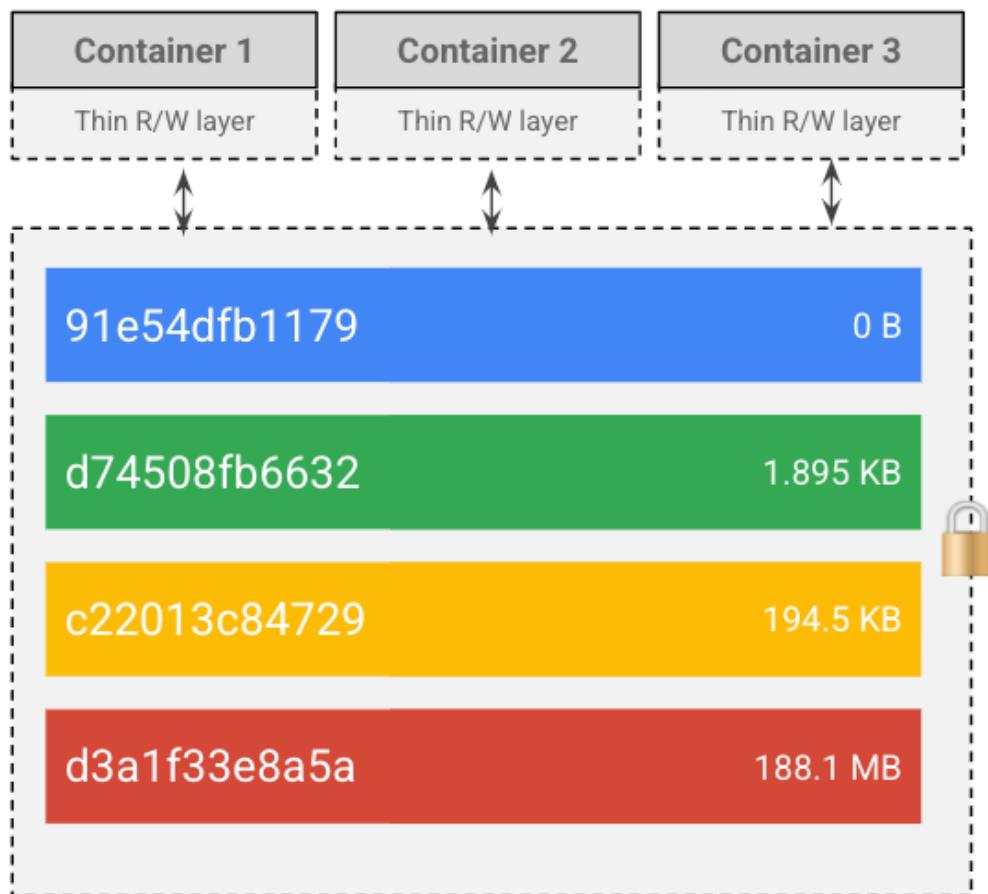


Figure 15.1 – Container structure



ubuntu:15.04

Figure 15.2 – Container layers

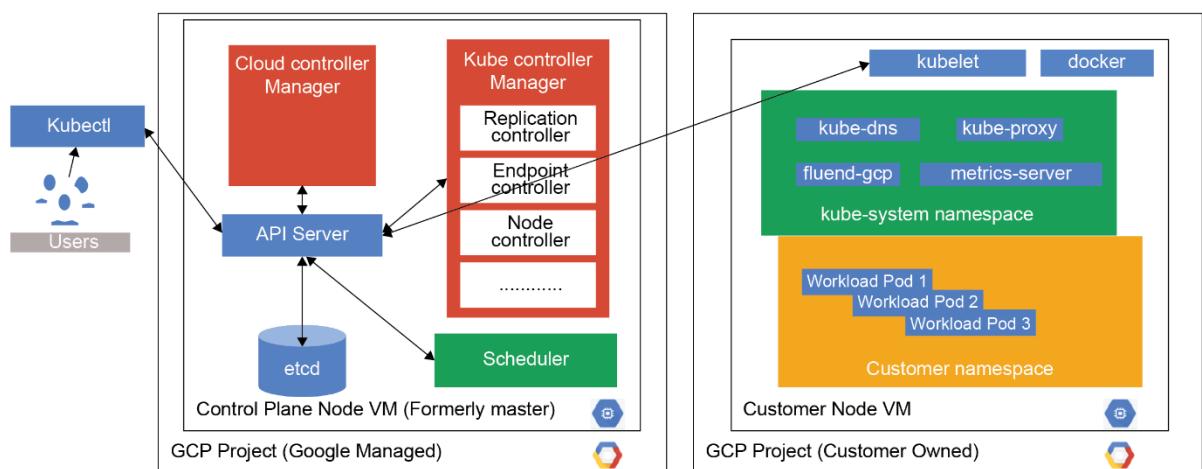


Figure 15.3 – GKE architecture

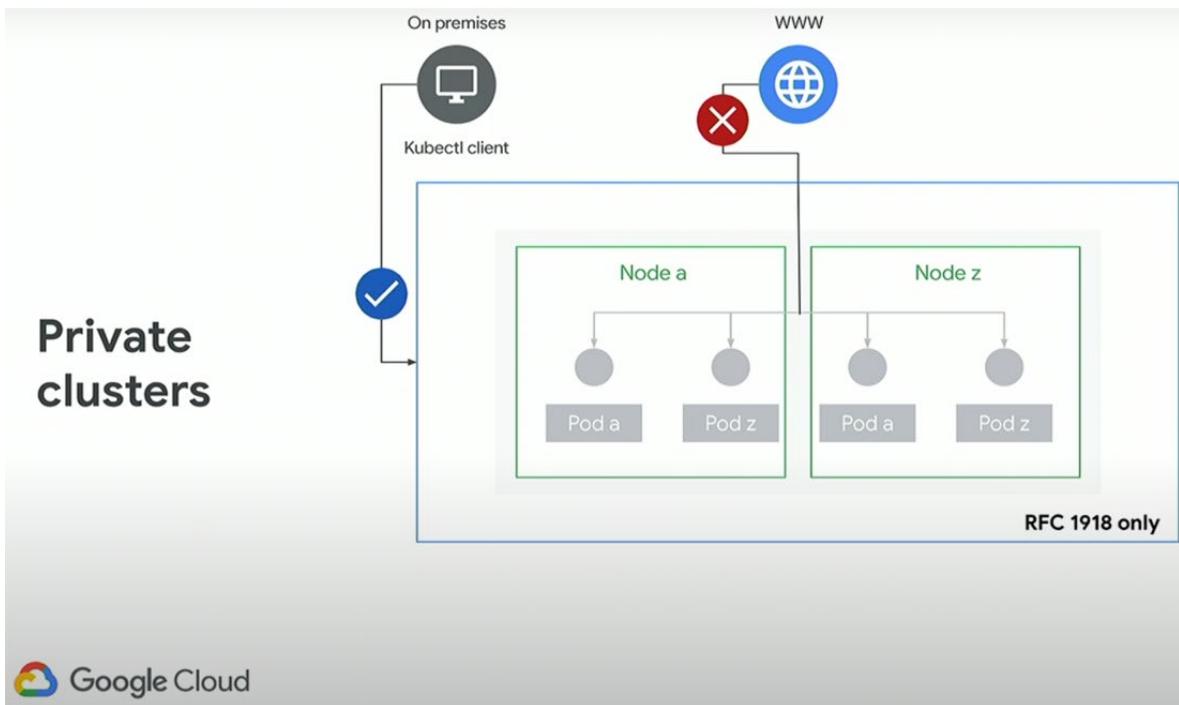


Figure 15.4 – Private clusters

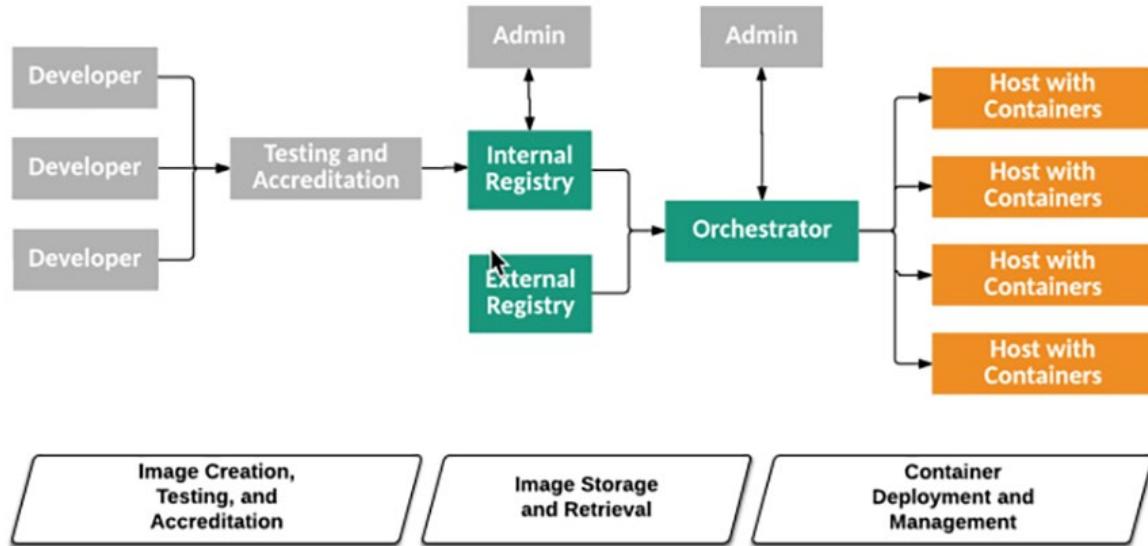


Figure 15.5 – Container pipeline

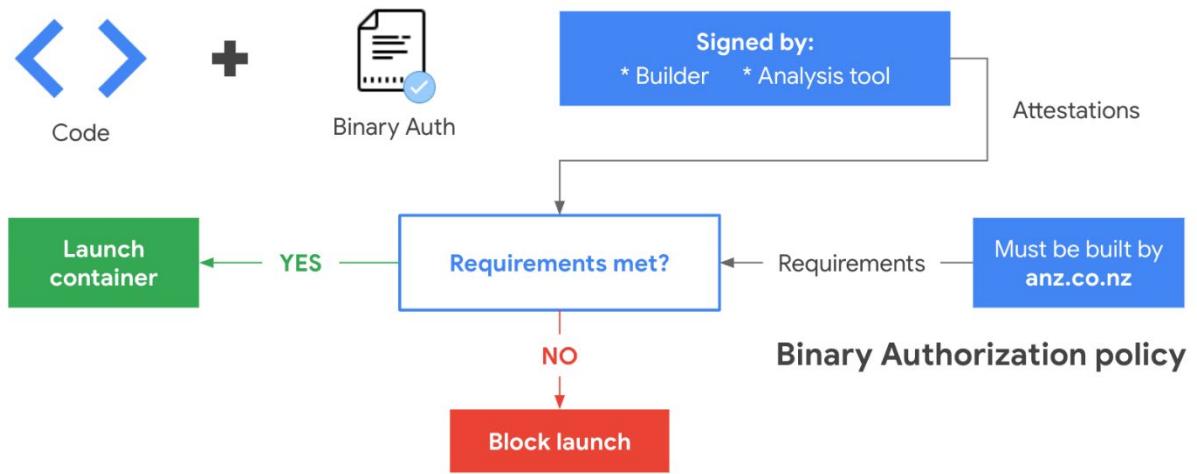


Figure 15.6 – Binary Authorization

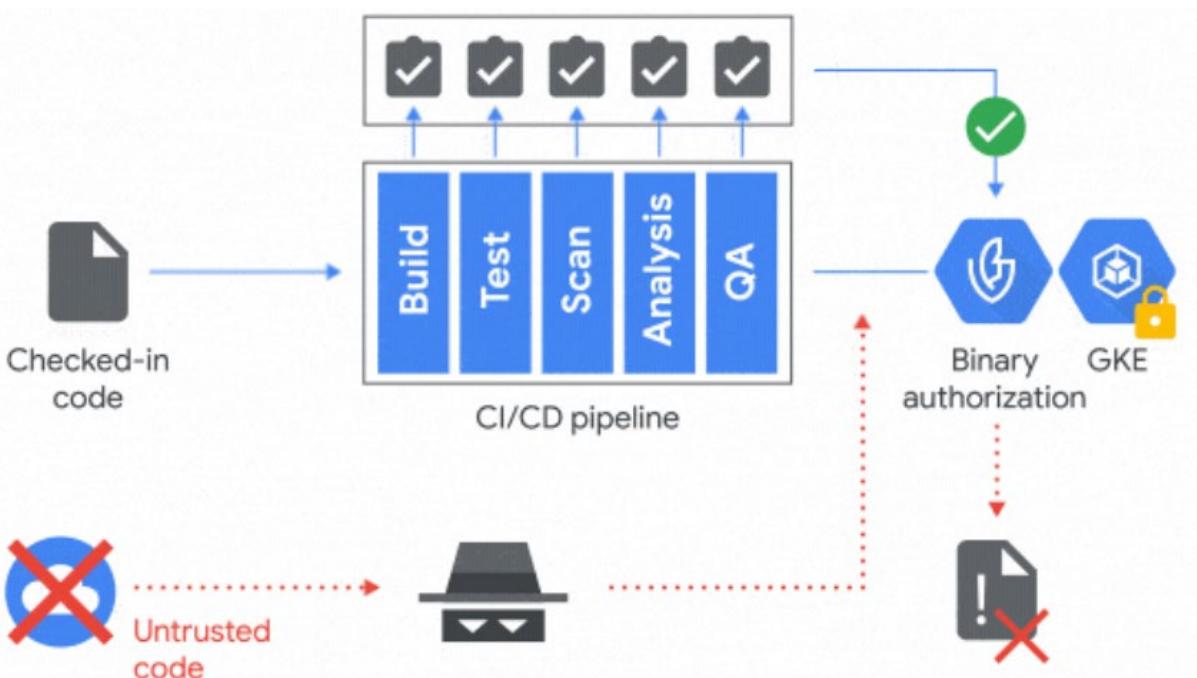


Figure 15.7 – Binary Authorization in the CI/CD pipeline