Official Google Cloud Certified Professional Cloud Security Engineer Exam Guide

Chapter 1: About the GCP Professional Cloud Security Engineer Exam

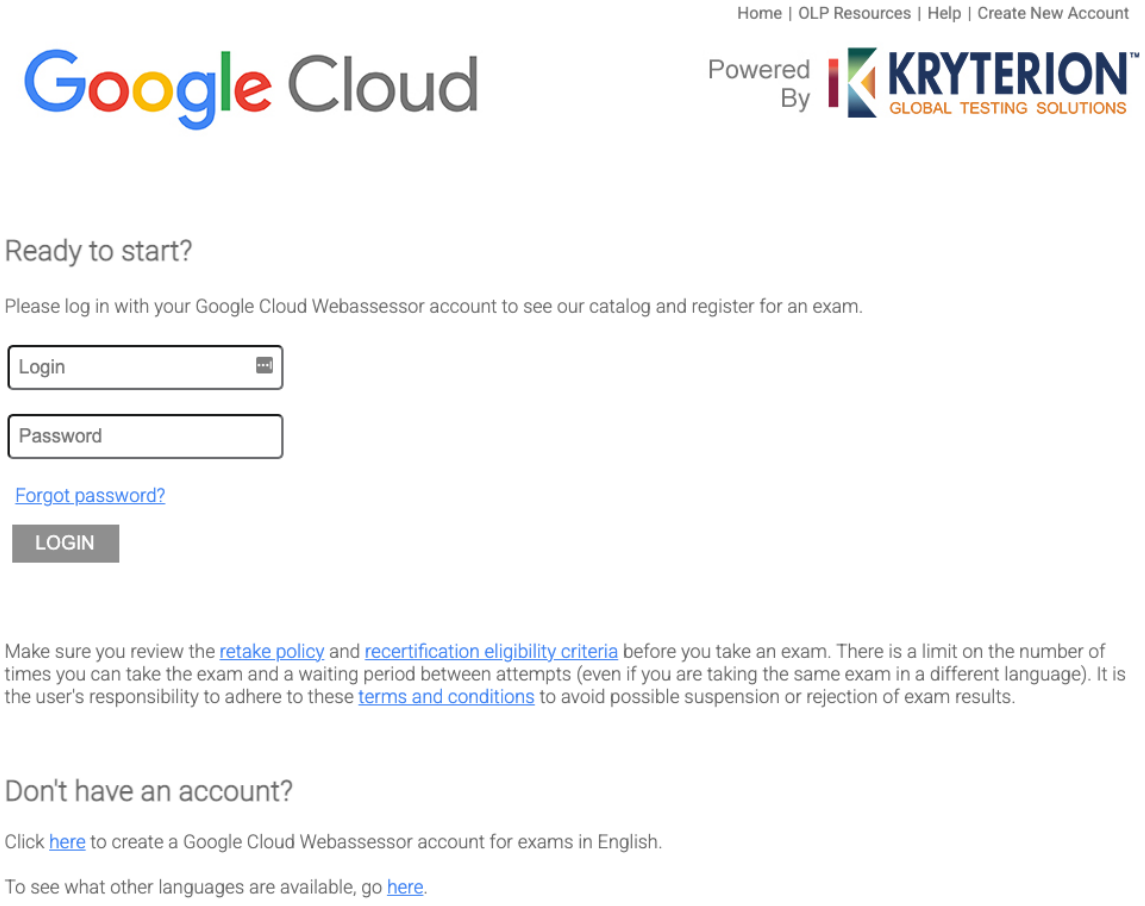


Figure 1.1 – Logging in to Webassessor

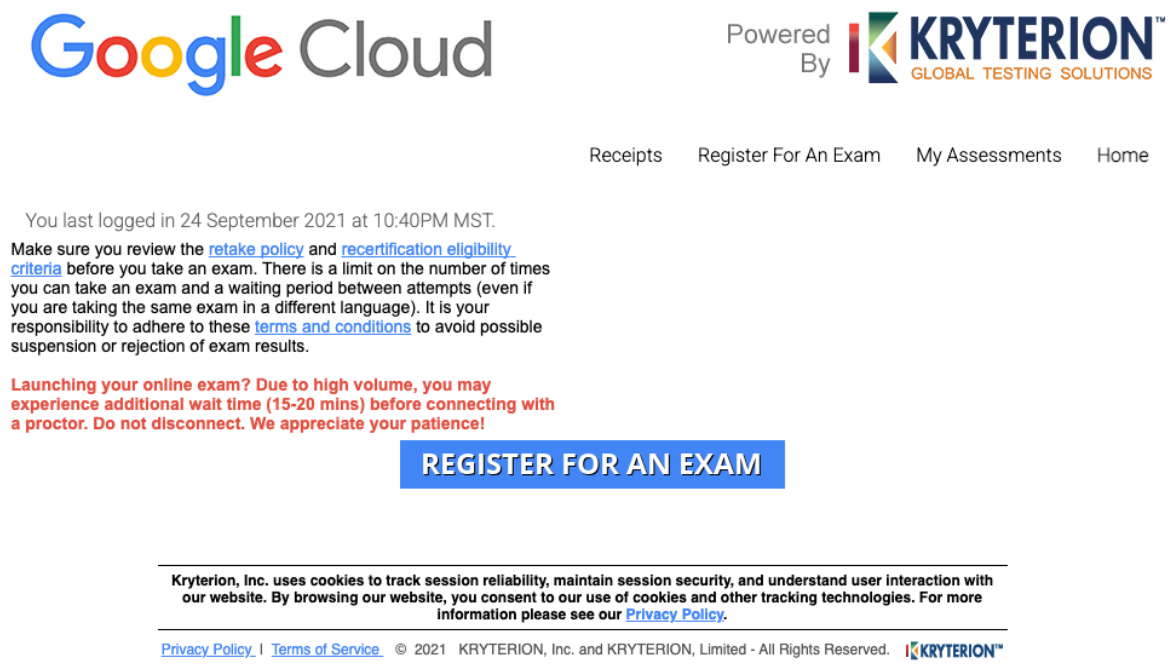


Figure 1.2 – Registration page

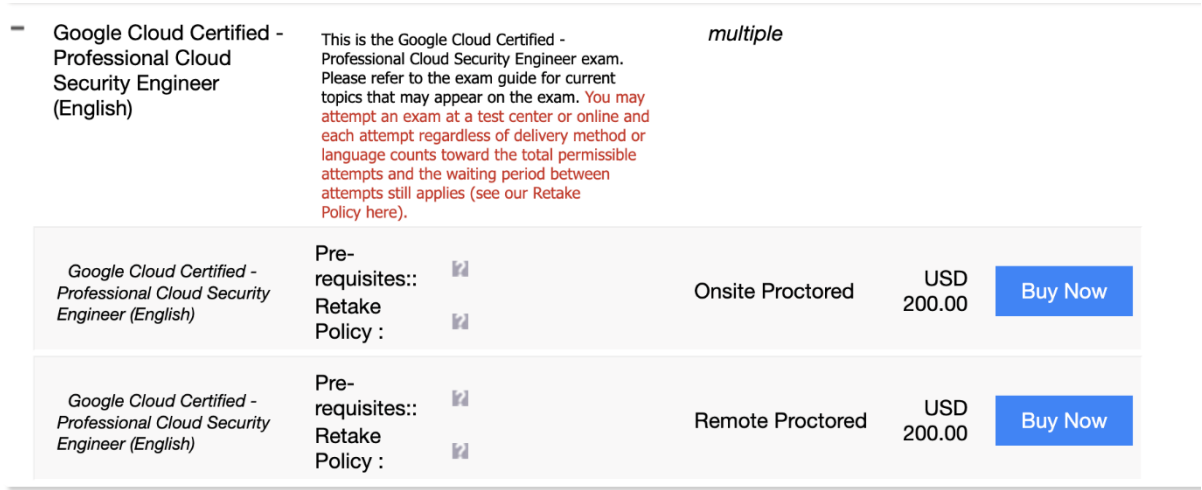


Figure 1.3 – Exam selection

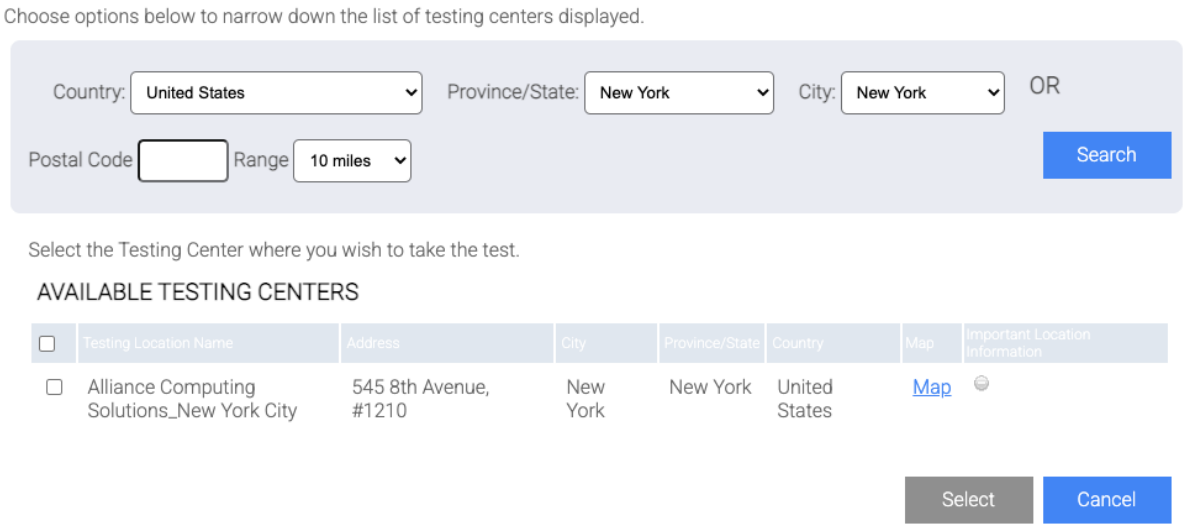


Figure 1.4 – Select a testing center

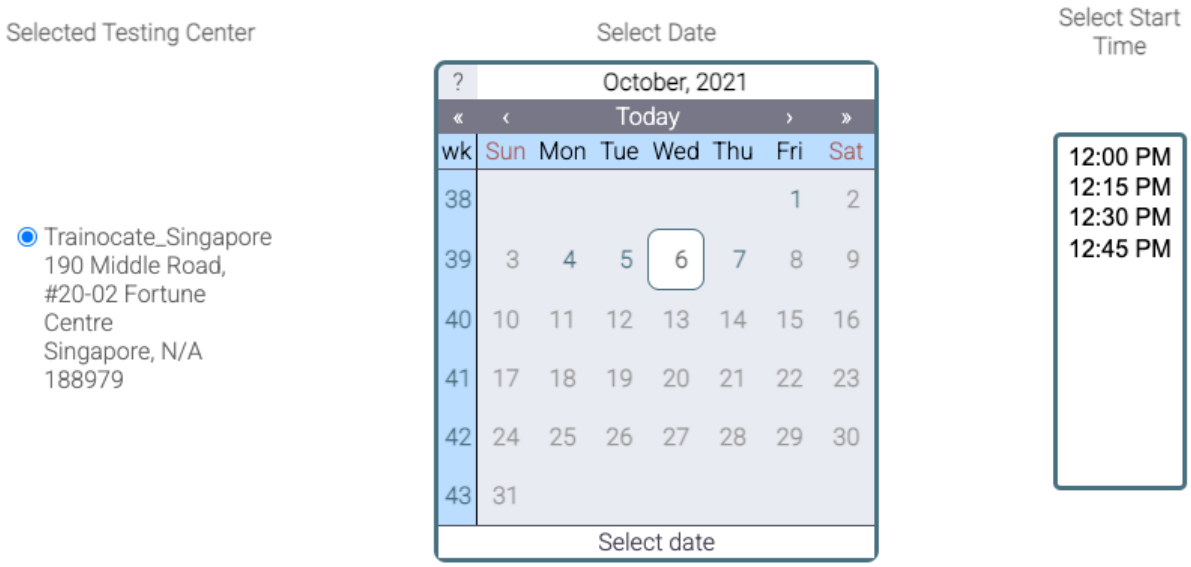


Figure 1.5 – Book a date and time for the exam

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

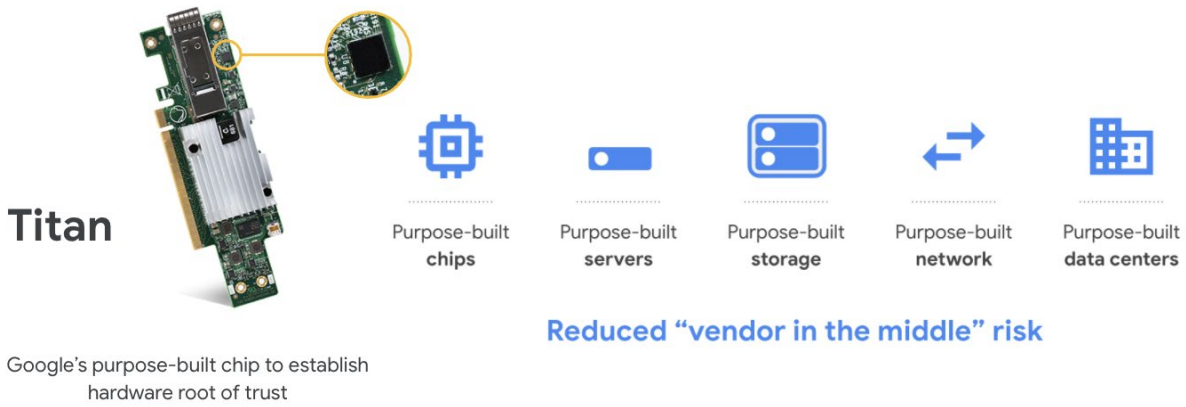


Figure 2.1 – End-to-end provenance and attestation

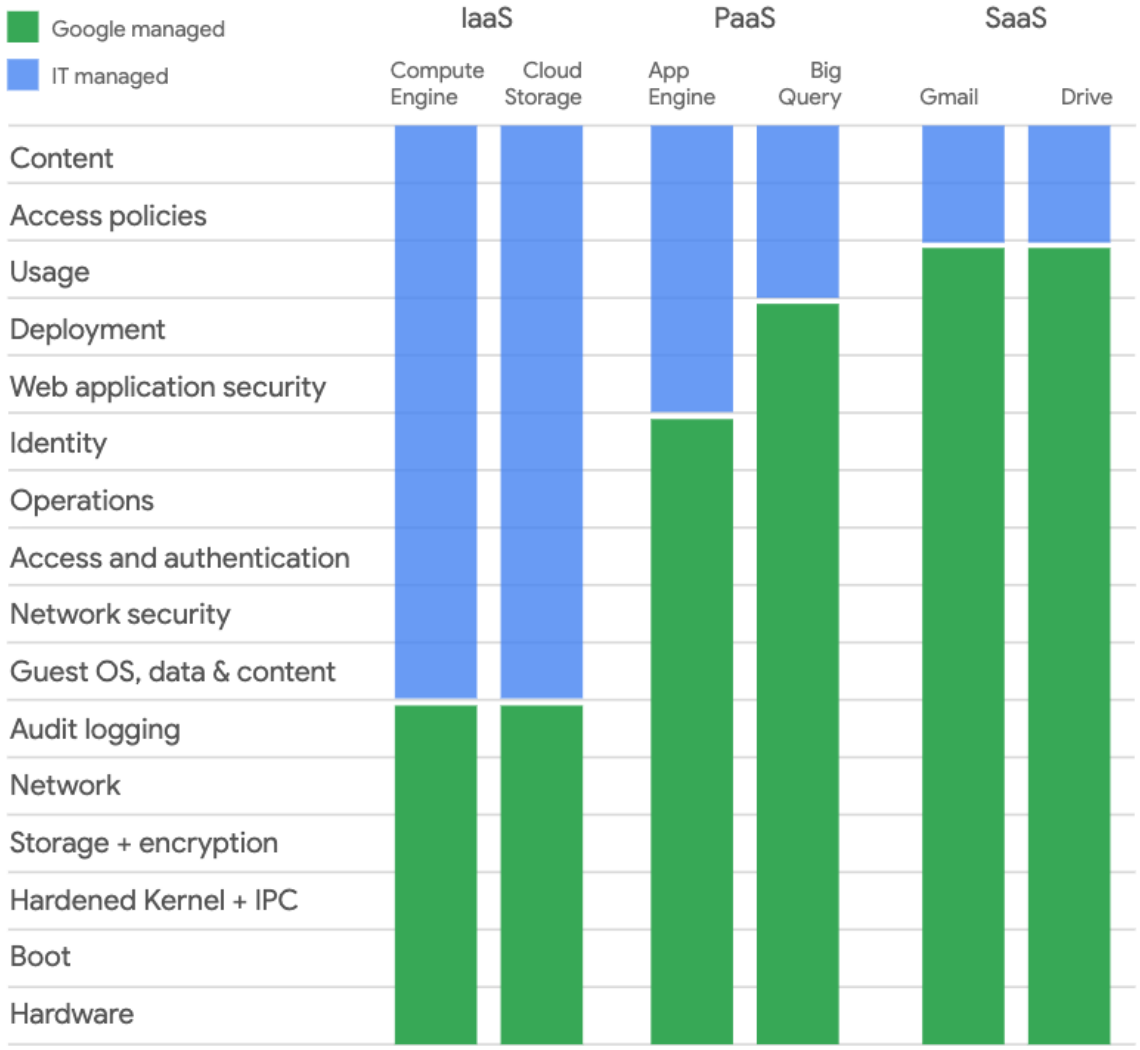


Figure 2.2 – Google Cloud's shared security responsibility (IaaS)

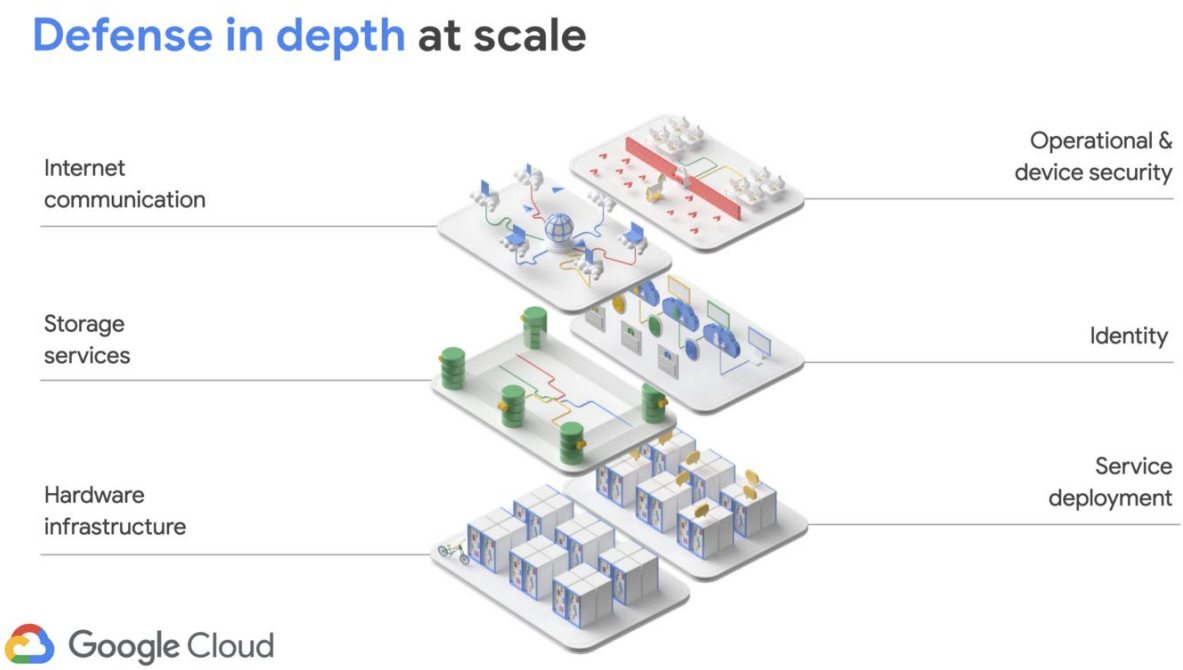


Figure 2.3 – Google defense in depth

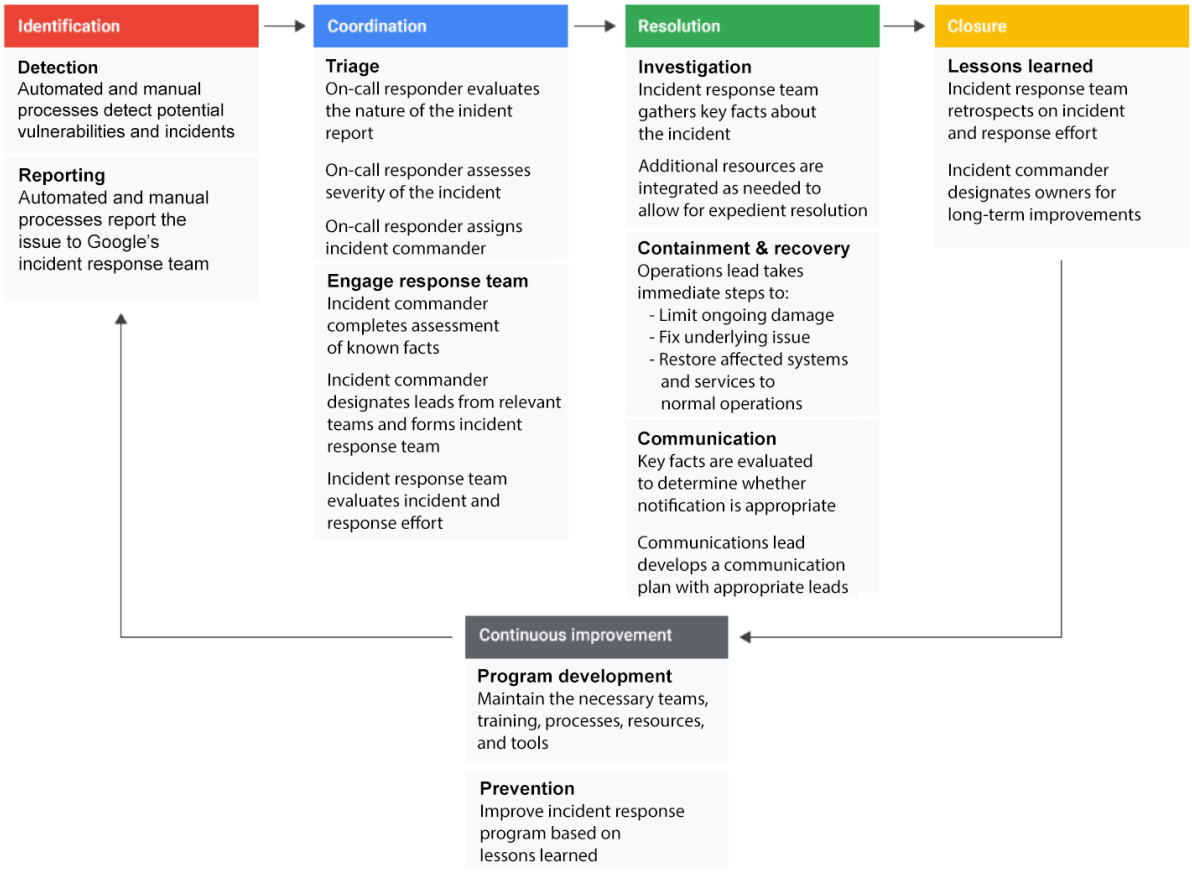


Figure 2.4 – Google Incident response workflow

Chapter 3: Trust and Compliance

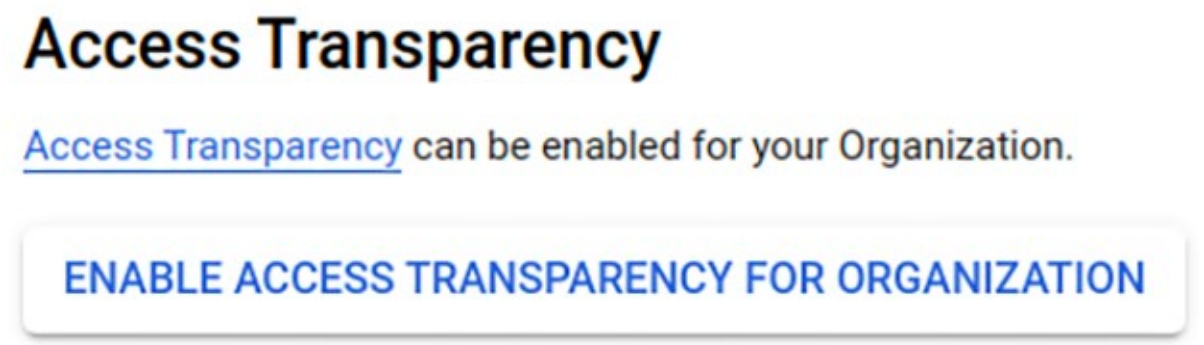


Figure 3.1 – Access Transparency enabled confirmation

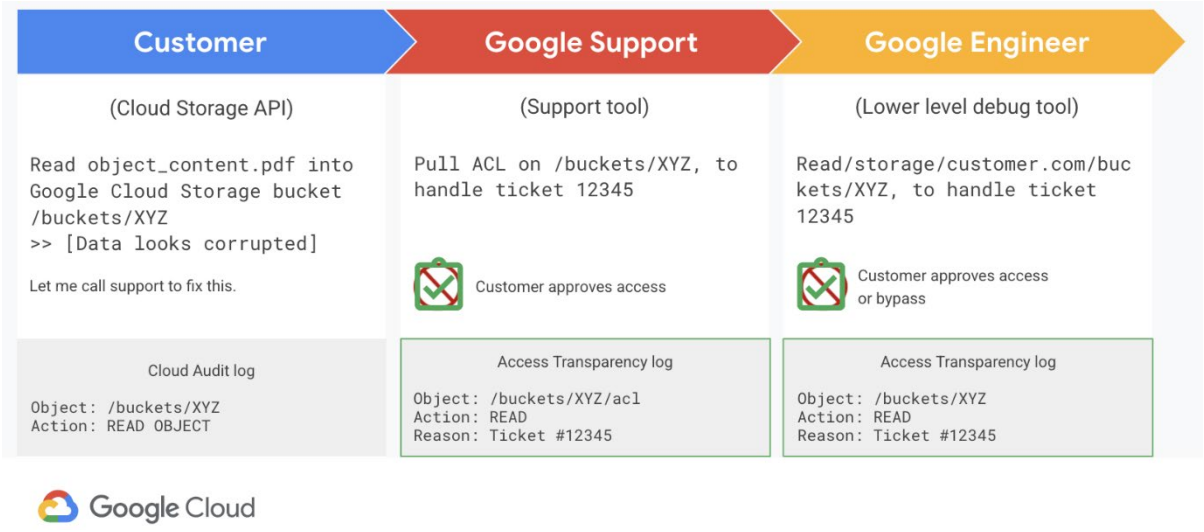


Figure 3.2 – Access Approval workflow

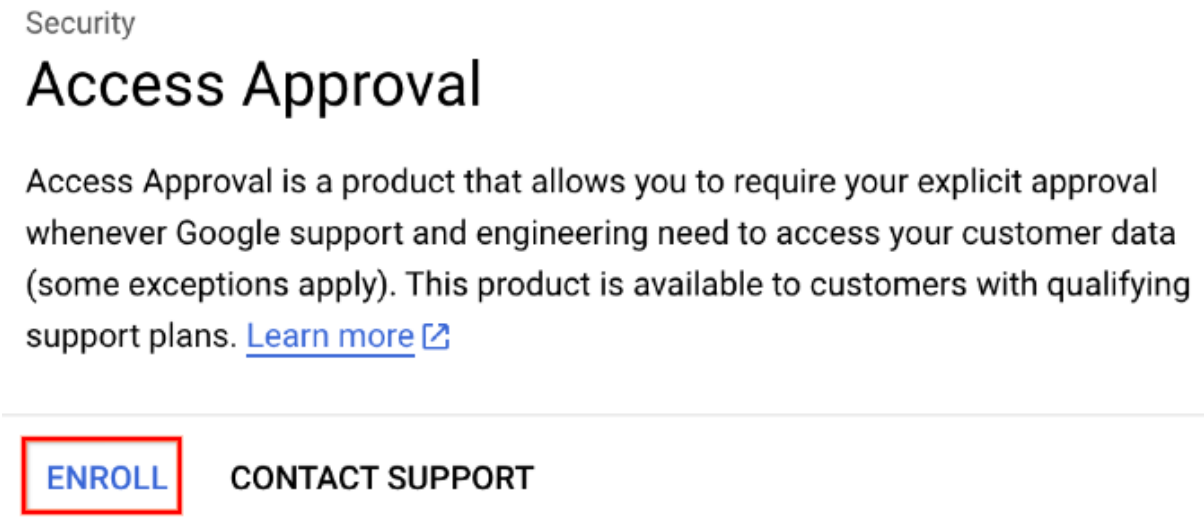


Figure 3.3 – Access Approval enrollment

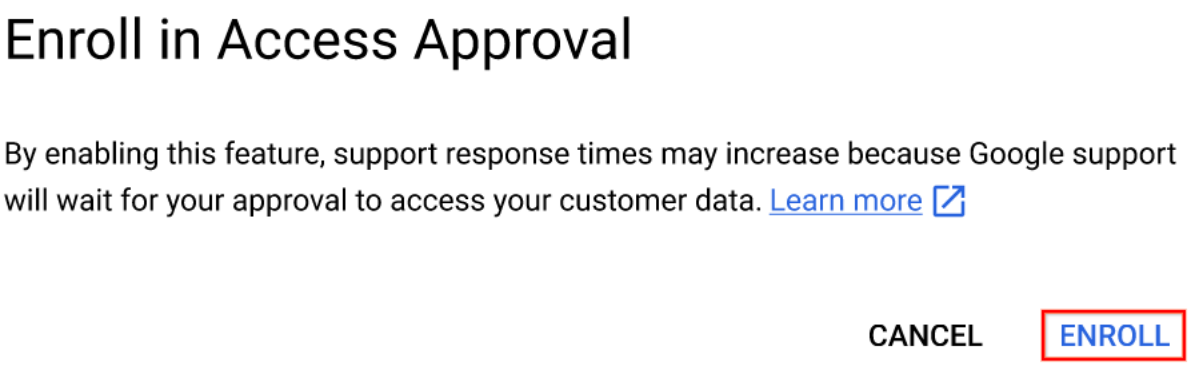


Figure 3.4 – Access Approval enrollment success

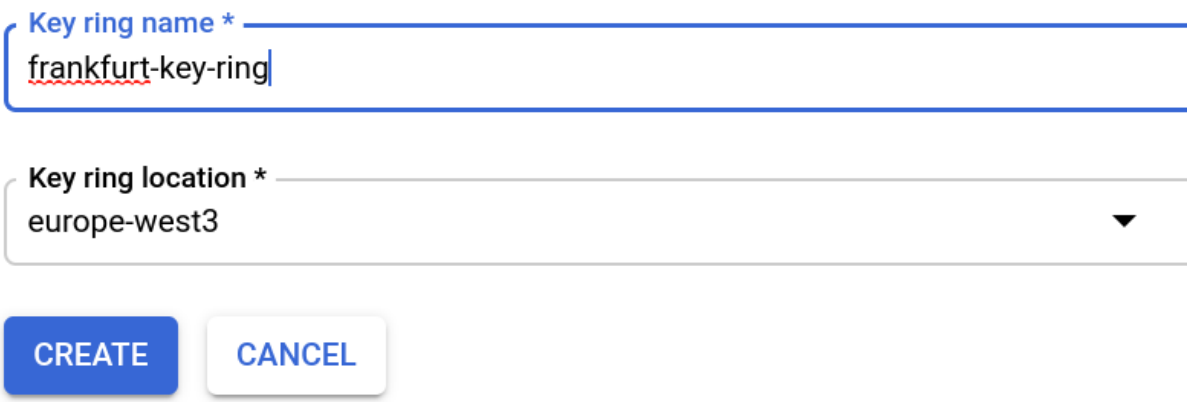


Figure 3.5 – Google Cloud KMS geo-location configuration for key ring

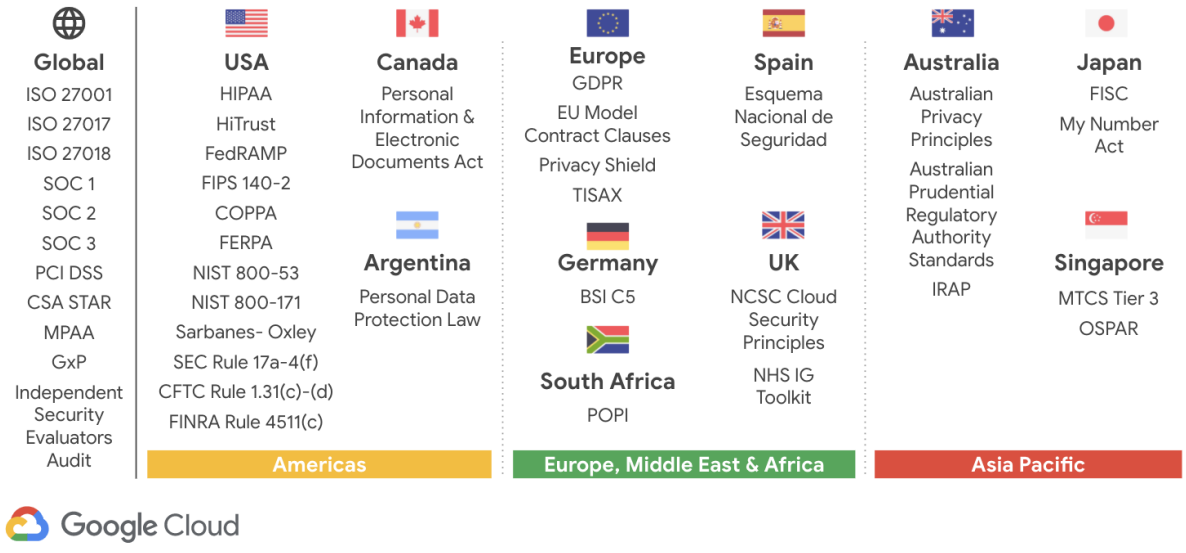


Figure 3.6 – Third-party certifications and regulatory compliance

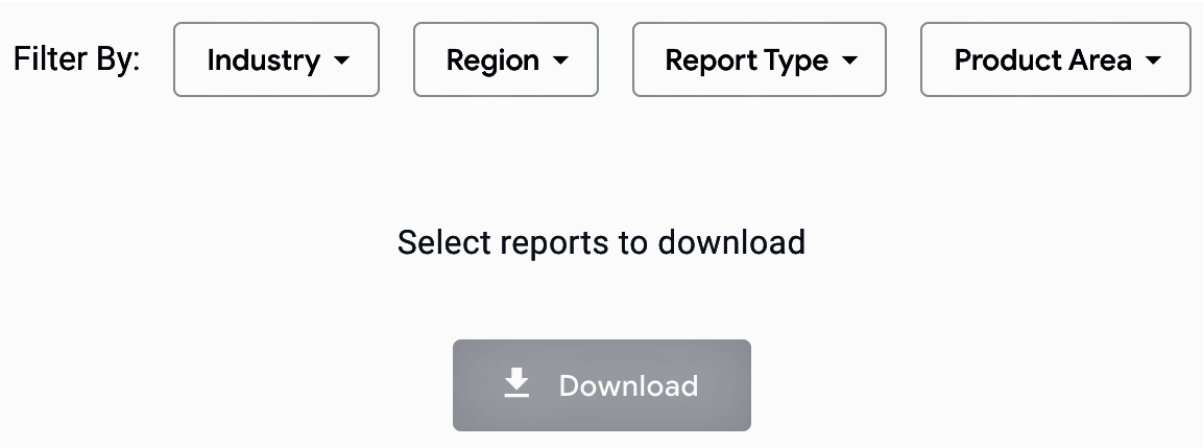


Figure 3.7 – Compliance Reports Manager

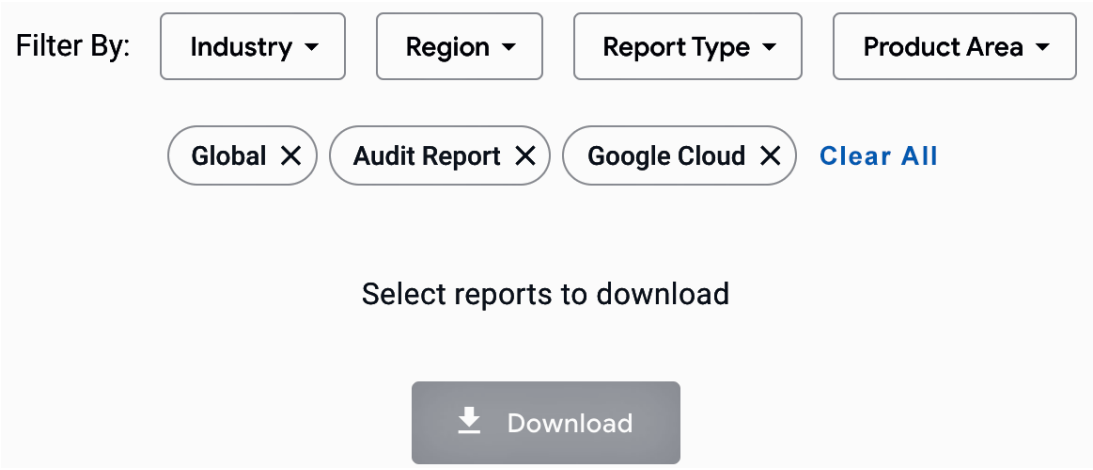


Figure 3.8 – Google Cloud Compliance Report Manager filter

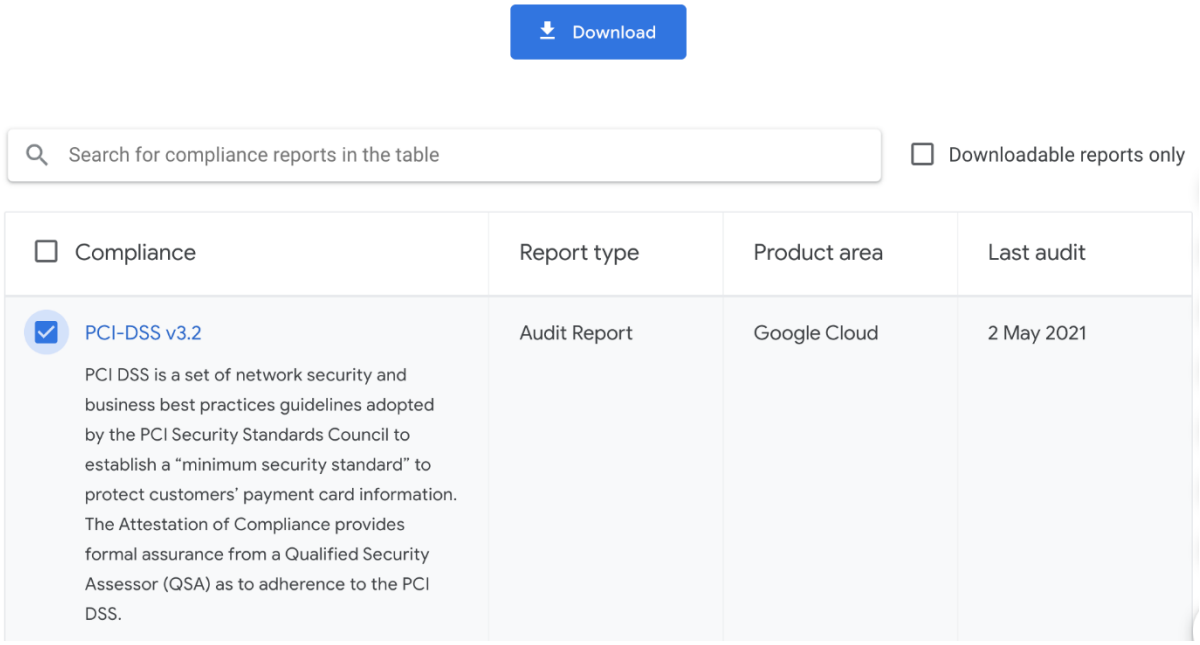


Figure 3.9 – Compliance manager: PCI-DSS report download

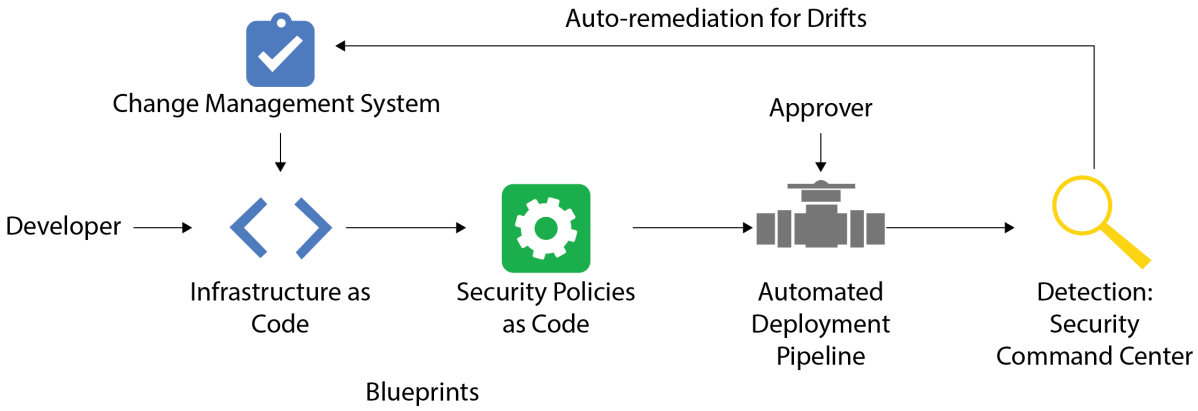


Figure 3.10 – Continuous compliance pipeline

Chapter 4: Resource Management

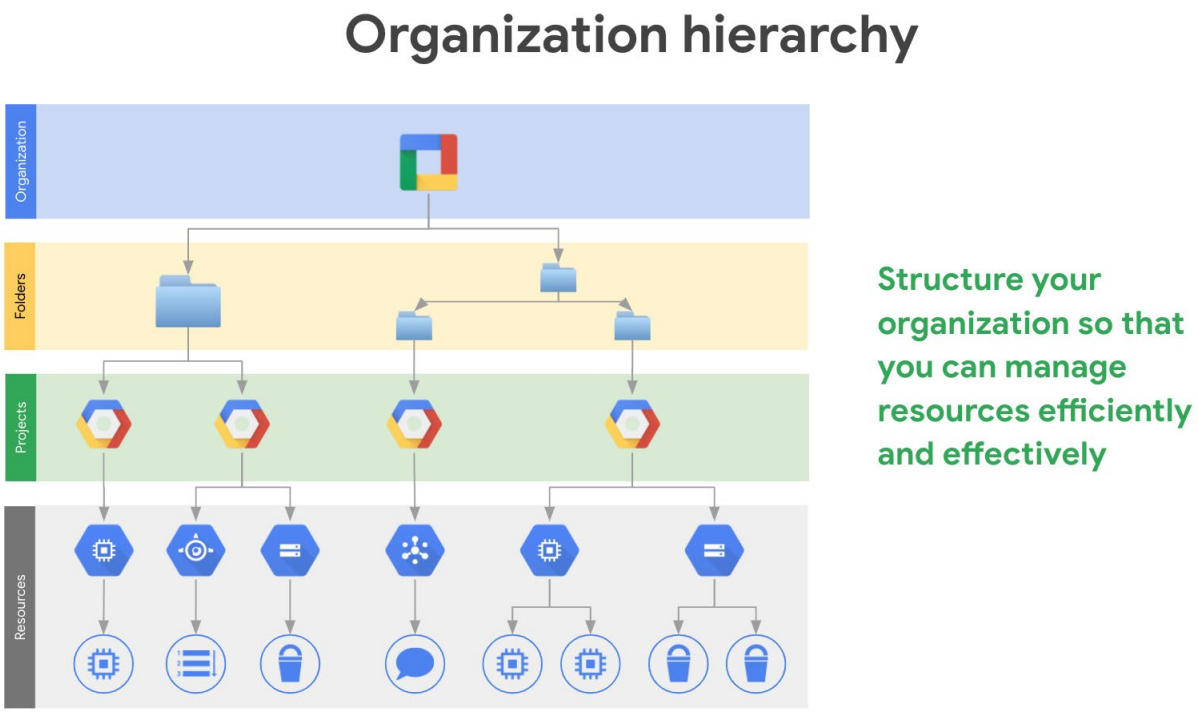


Figure 4.1 – Organization hierarchy

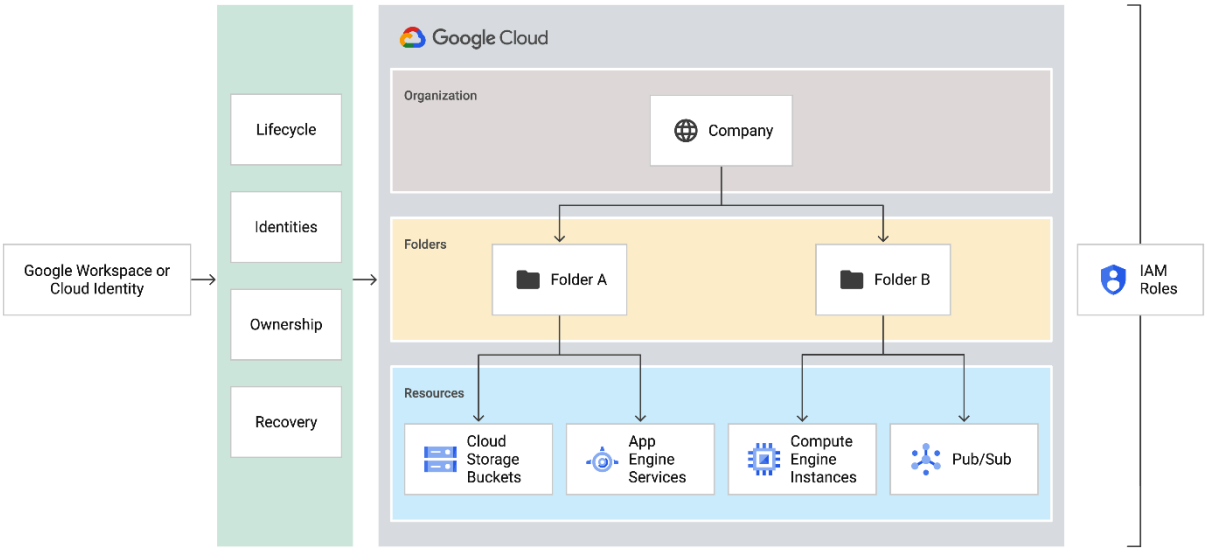


Figure 4.2 – Organizations

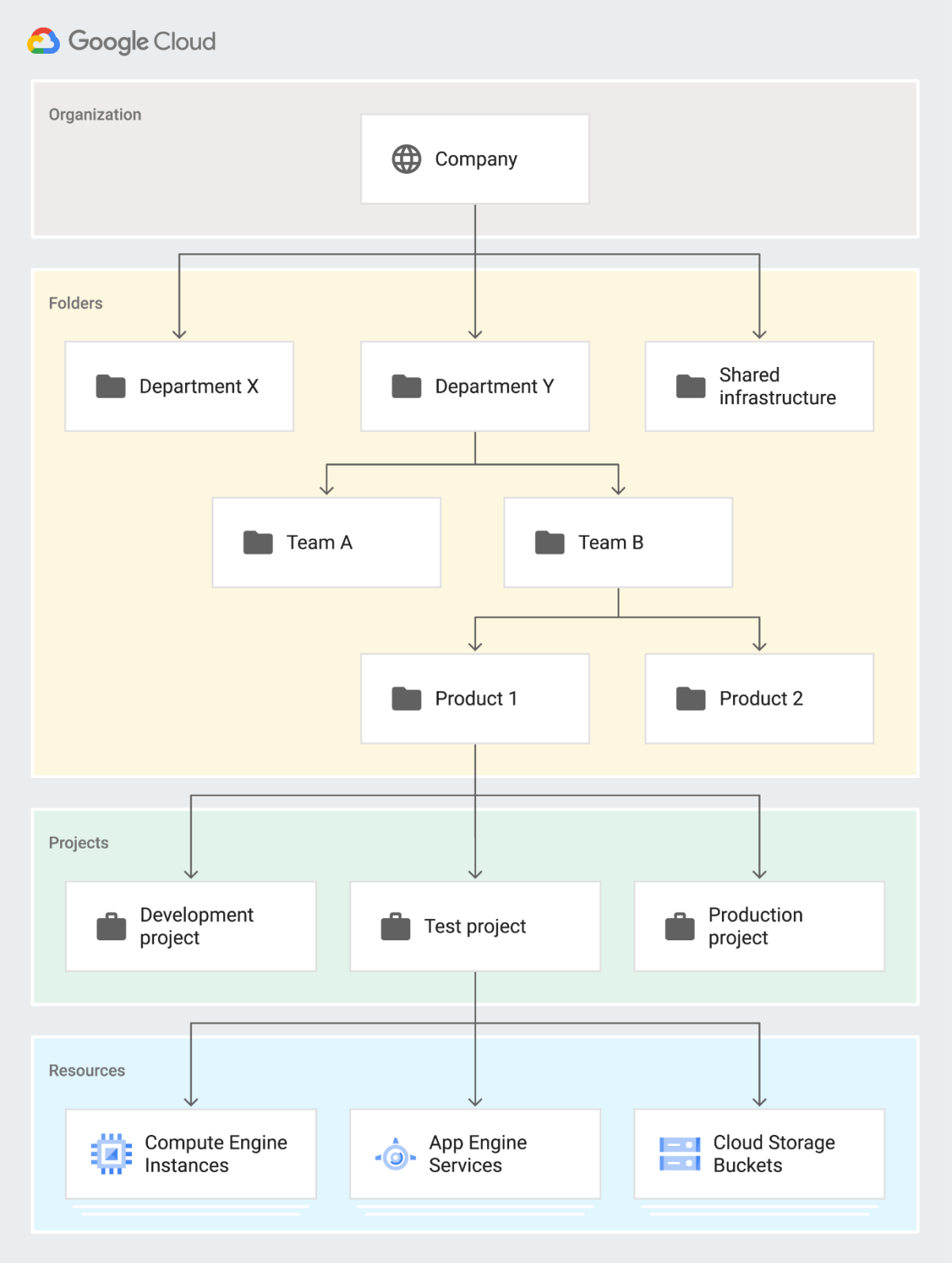


Figure 4.3 – Example enterprise organization

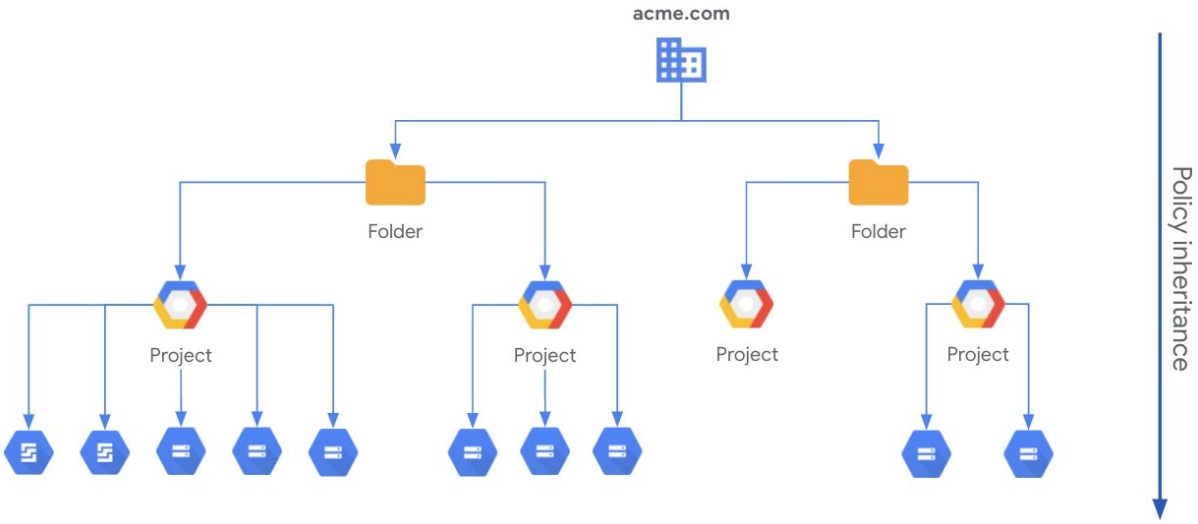


Figure 4.4 – IAM policy inheritance

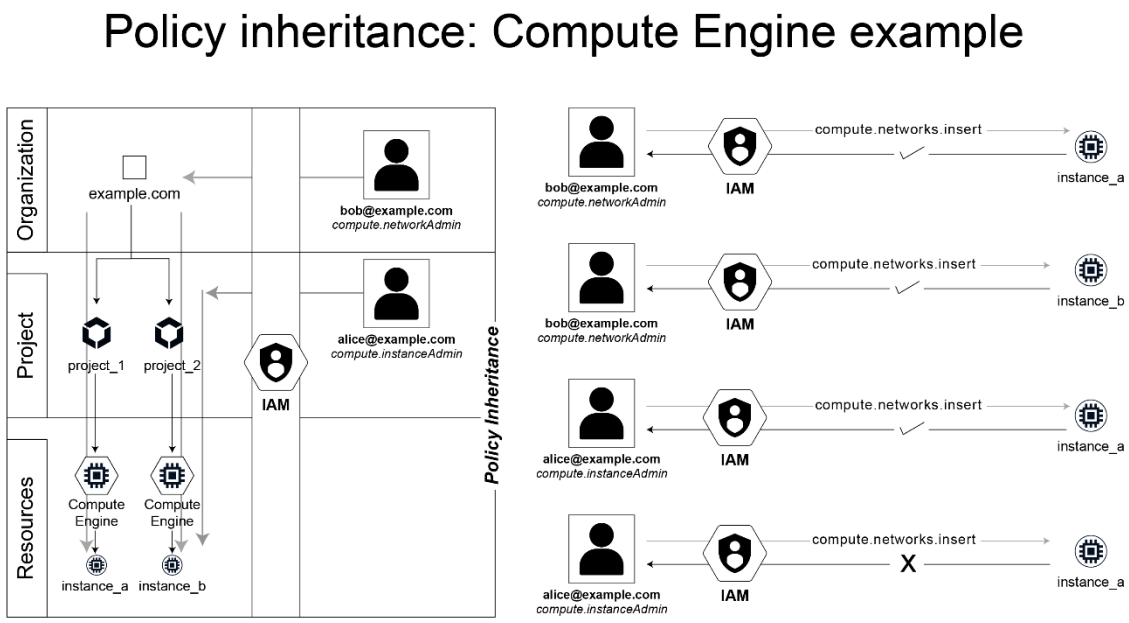


Figure 4.5 – IAM policy inheritance—Compute Engine

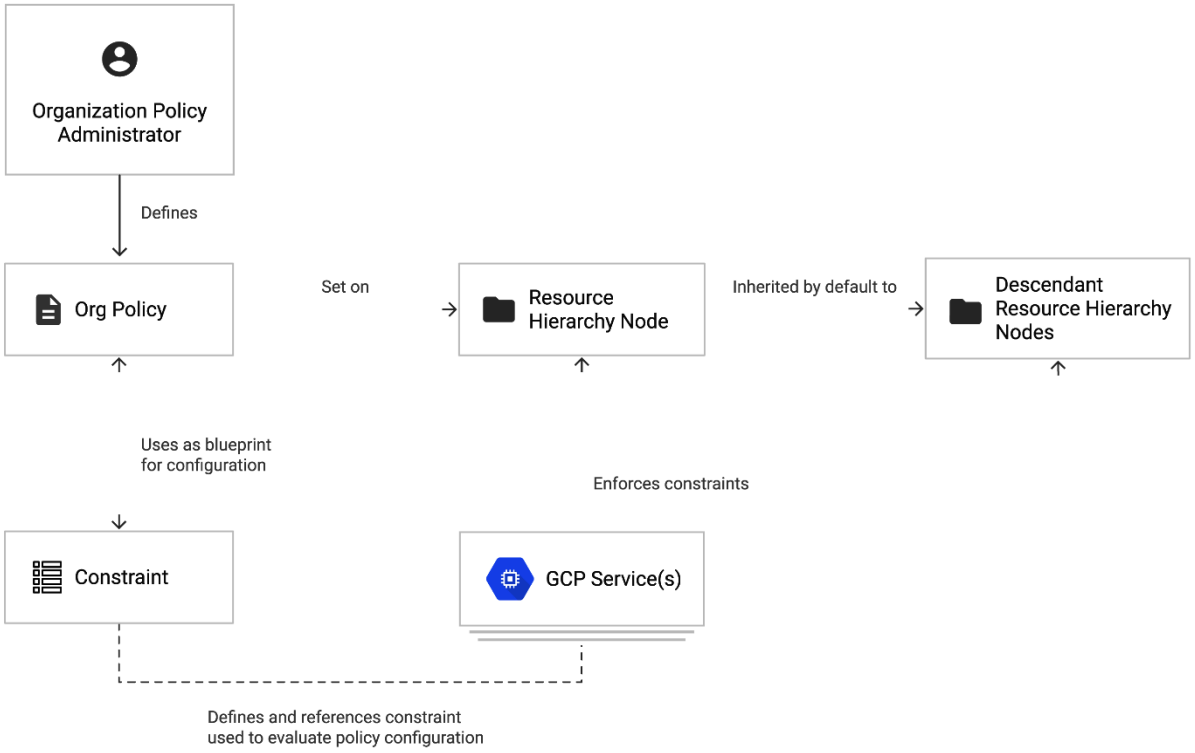


Figure 4.6 – Organization policy

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

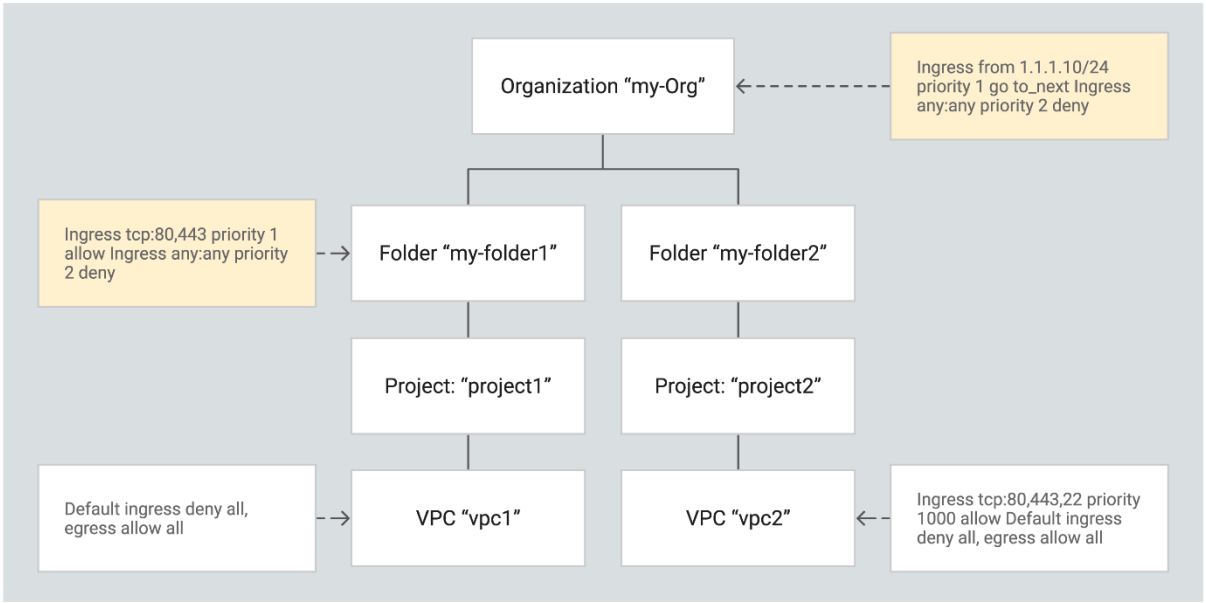


Figure 4.9 – Hierarchical firewall policy inheritance

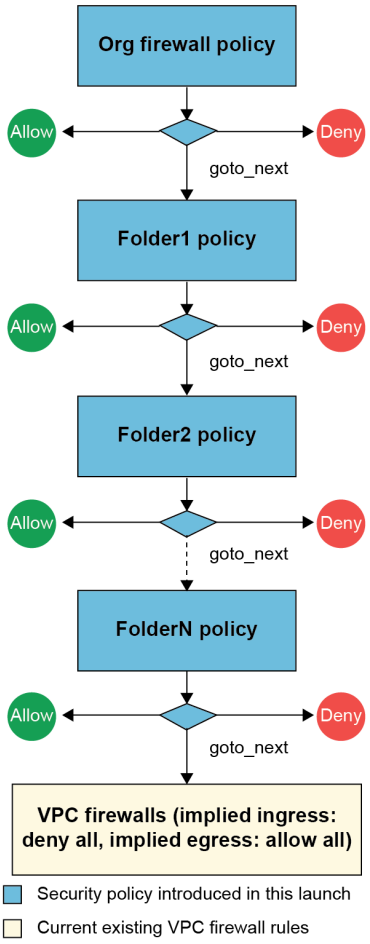


Figure 4.10 – Hierarchical firewall policy evaluation

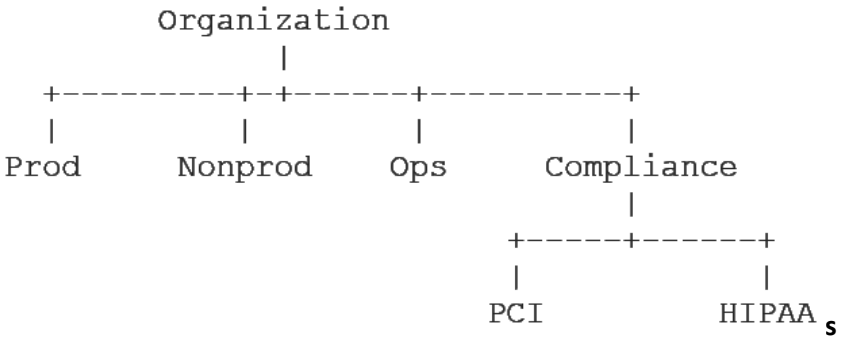


Figure 4.11 – Example organization structure

Chapter 5: Understanding Google Cloud Identity

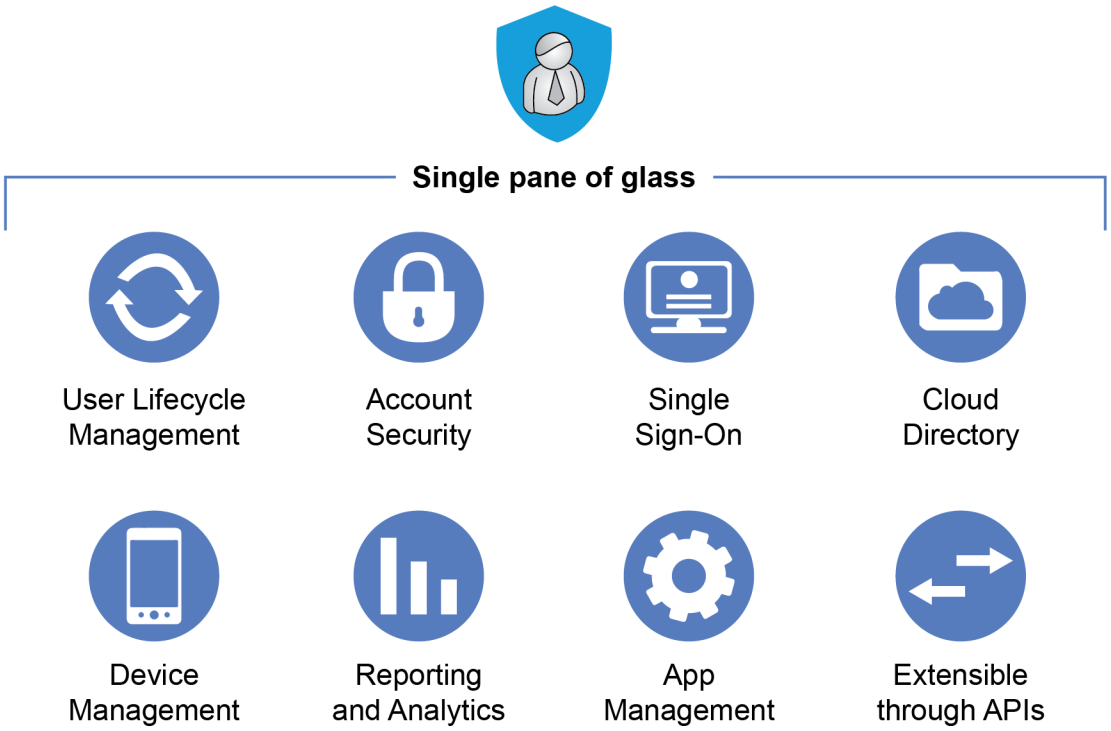


Figure 5.1 – Google Cloud Identity features

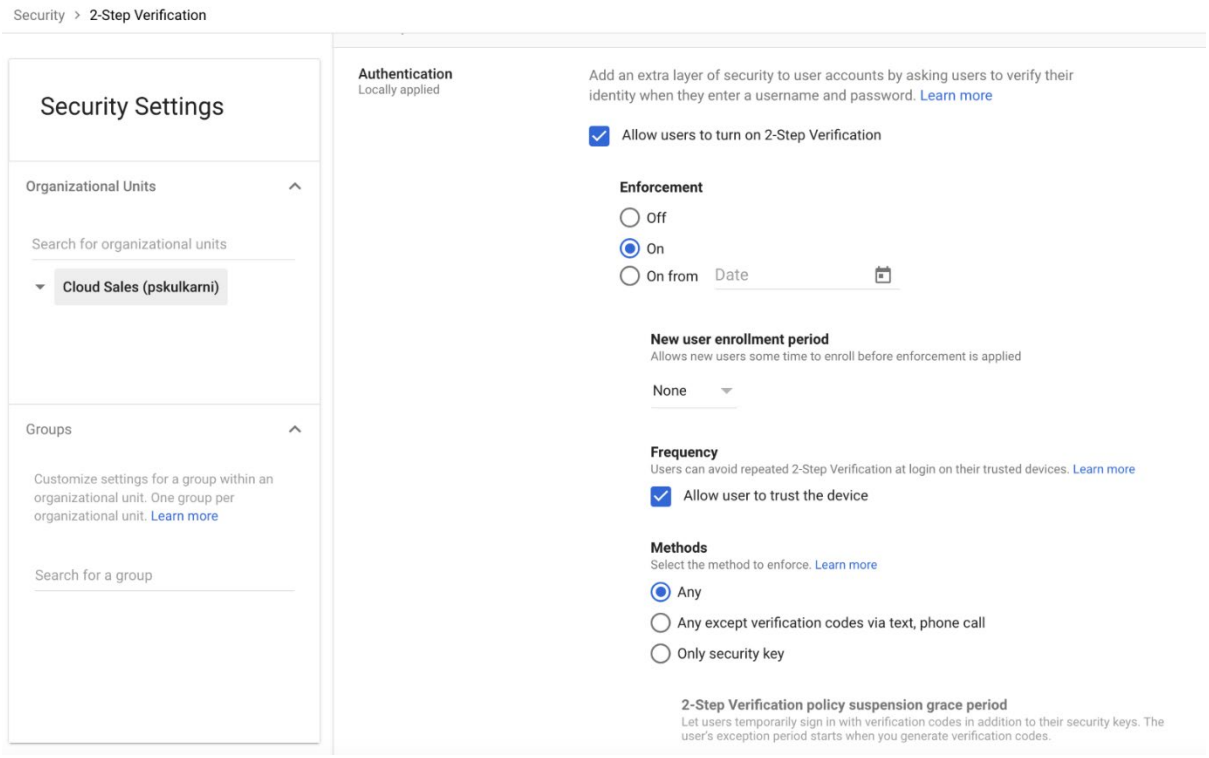


Figure 5.2 – Account security (2SV)

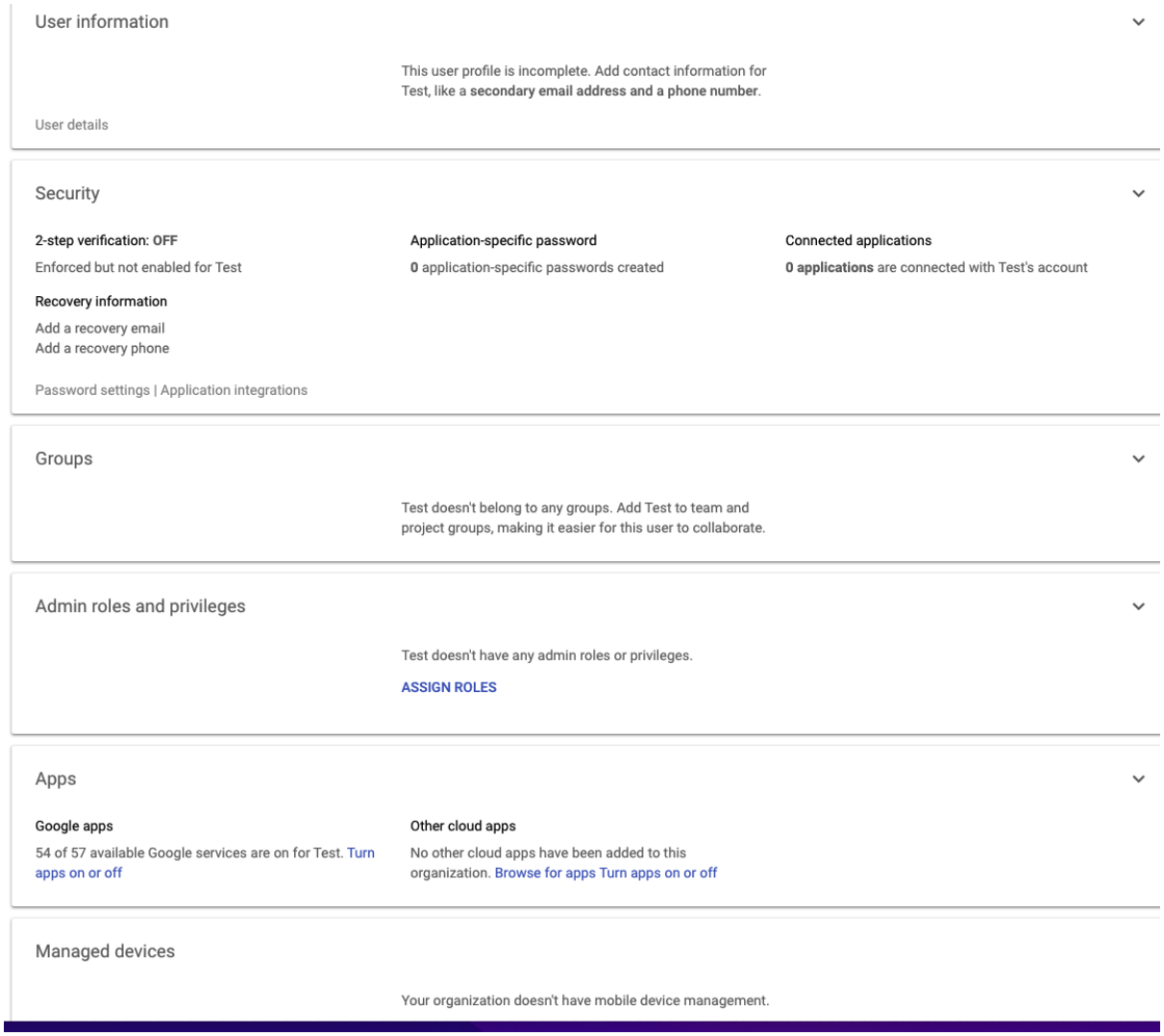


Figure 5.3 – Cloud Identity – user details

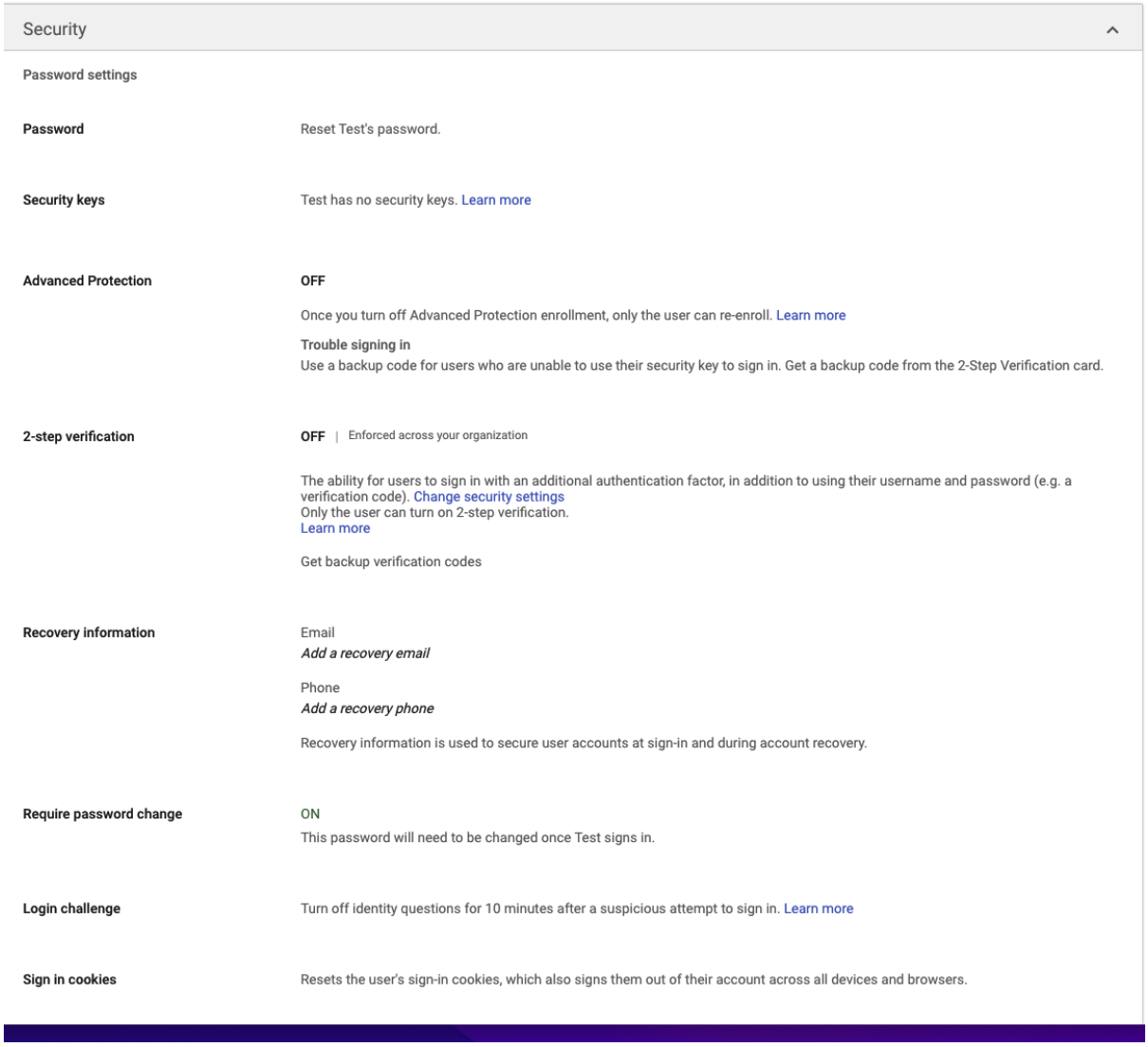


Figure 5.4 – Cloud Identity – user security settings

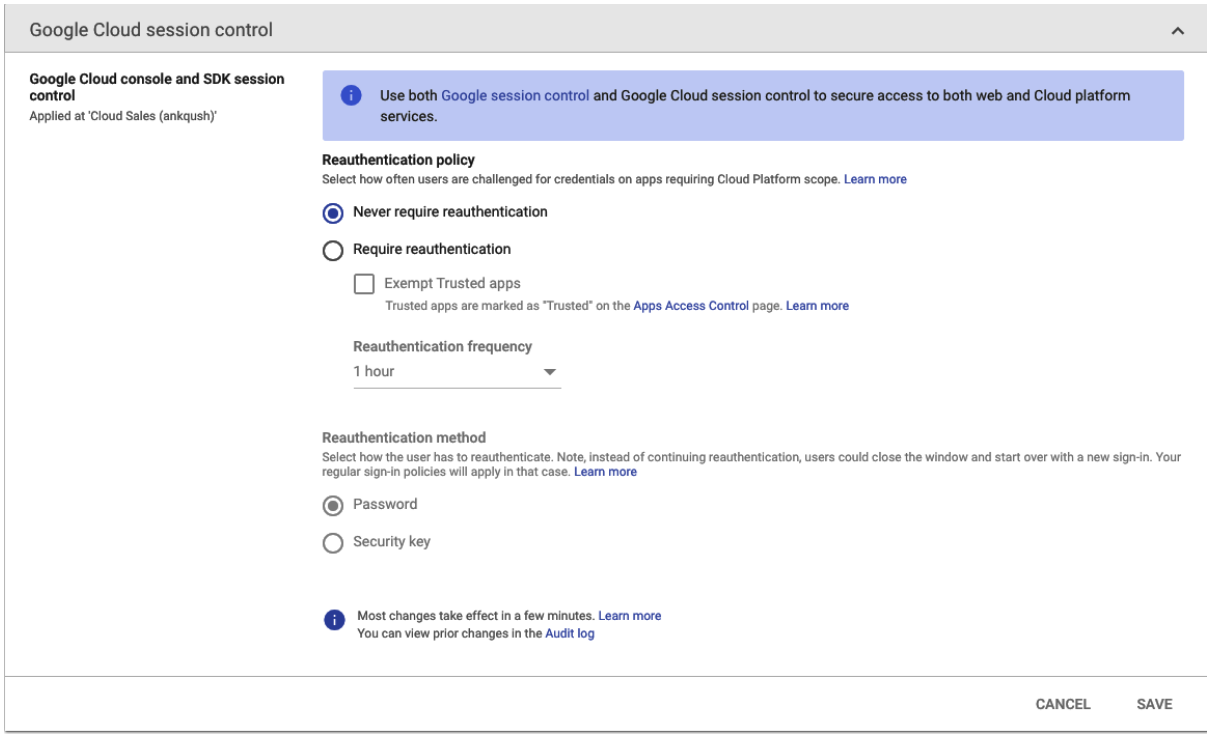


Figure 5.5 – Google Cloud session control

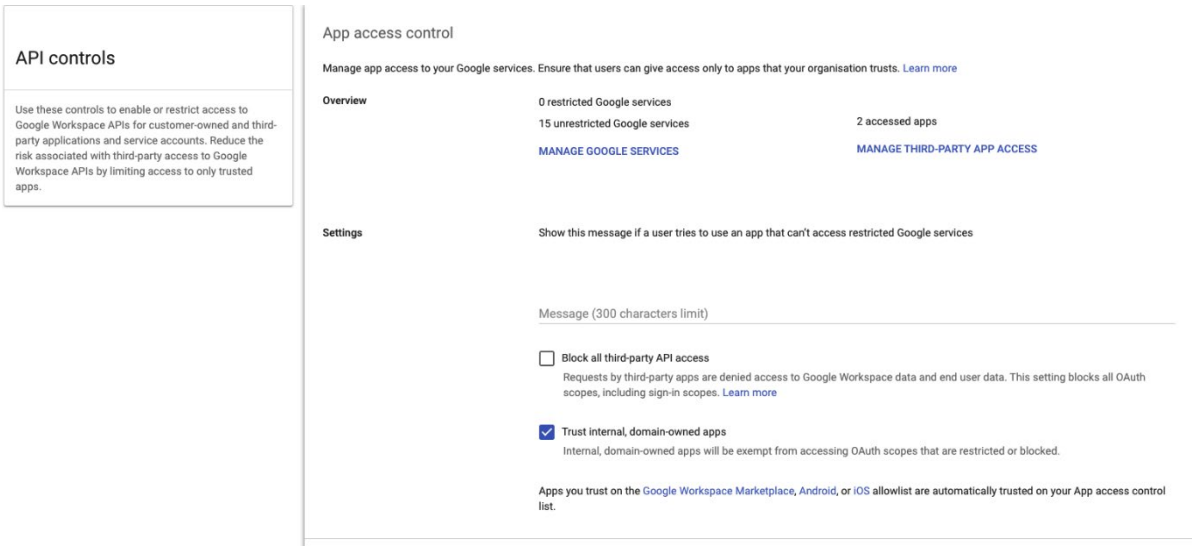


Figure 5.6 – Managing trusted third-party applications

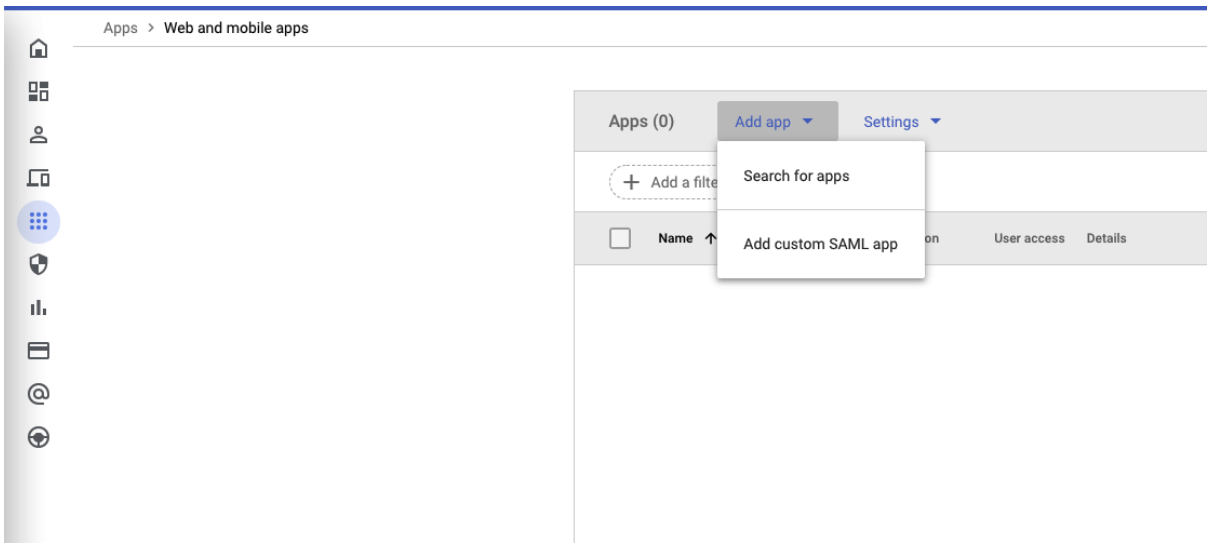


Figure 5.7 – Cloud Identity – Add custom SAML app

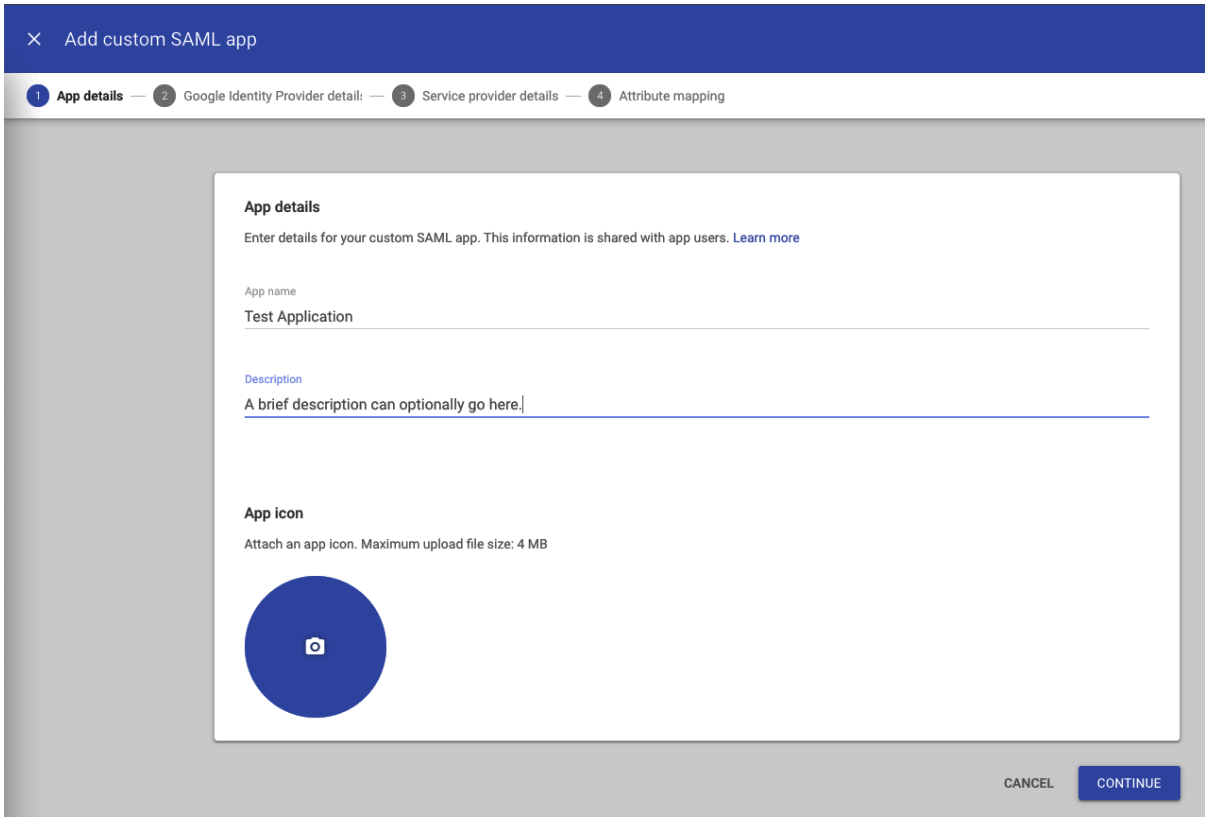


Figure 5.8 – Configure your custom SAML app

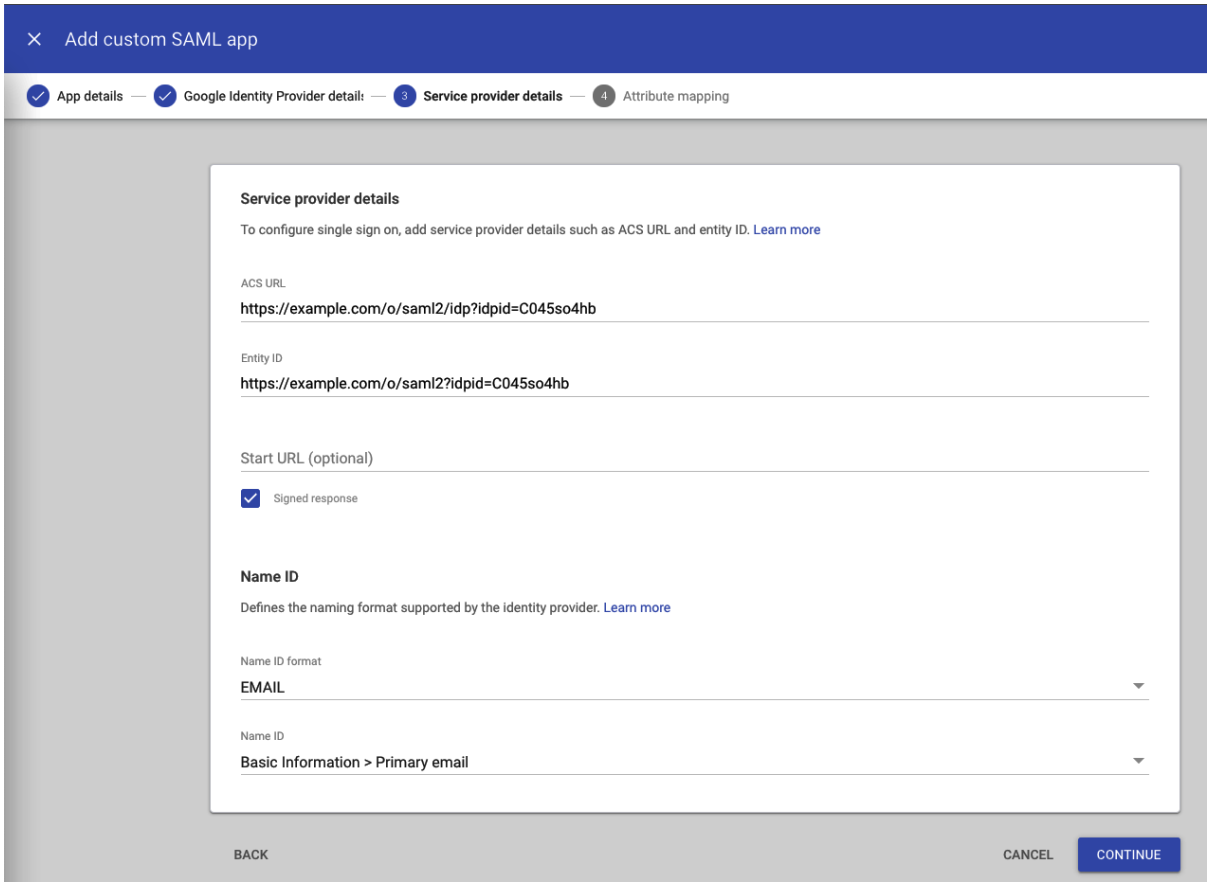


Figure 5.9 – SAML service provider details

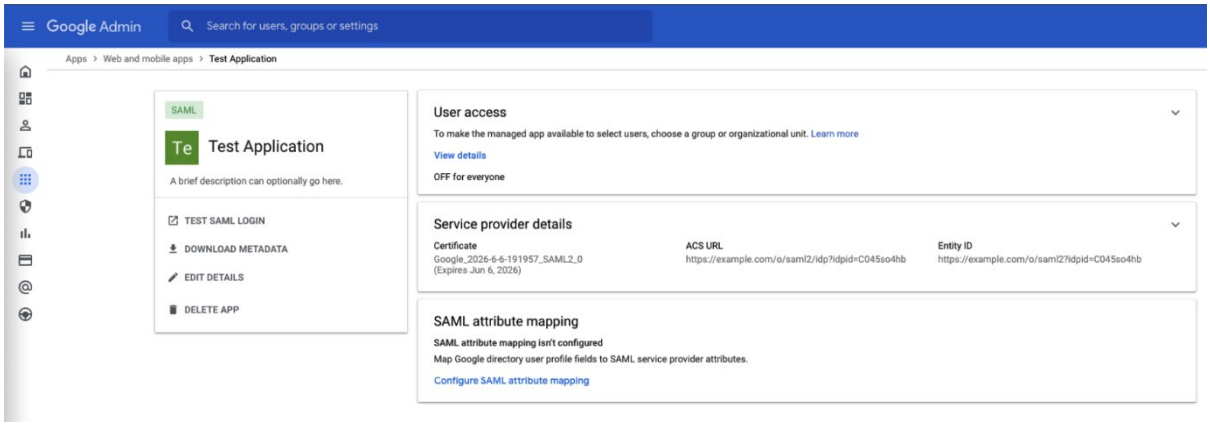


Figure 5.10 – App details page

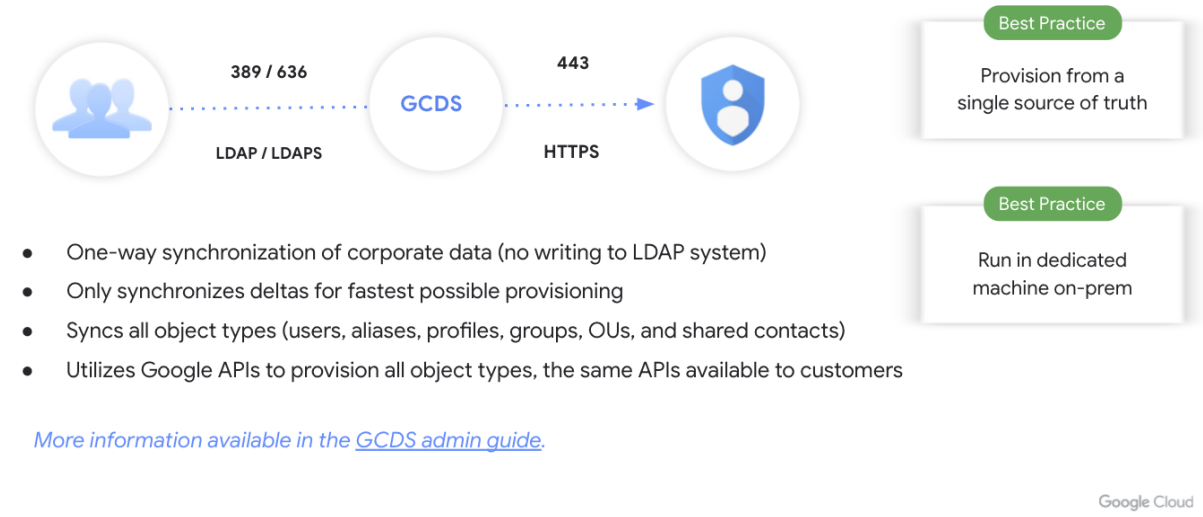


Figure 5.11 – The workings of GCDS

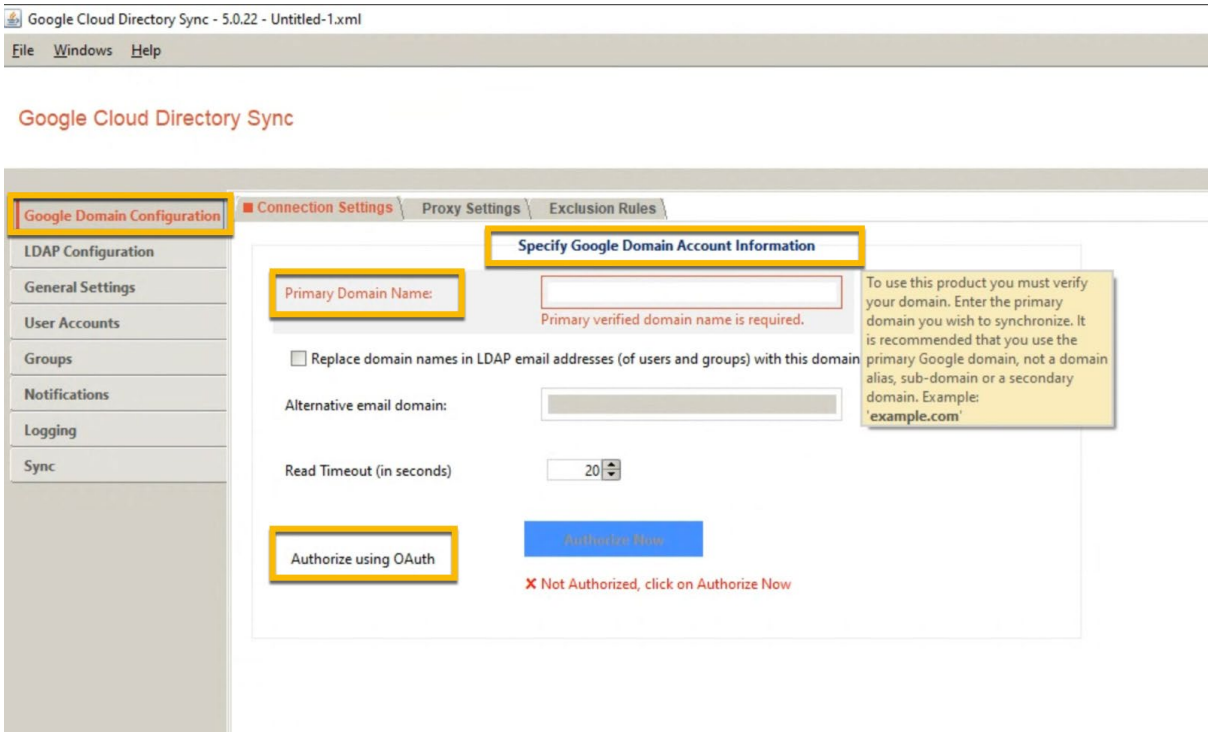


Figure 5.12 – Google Domain configuration

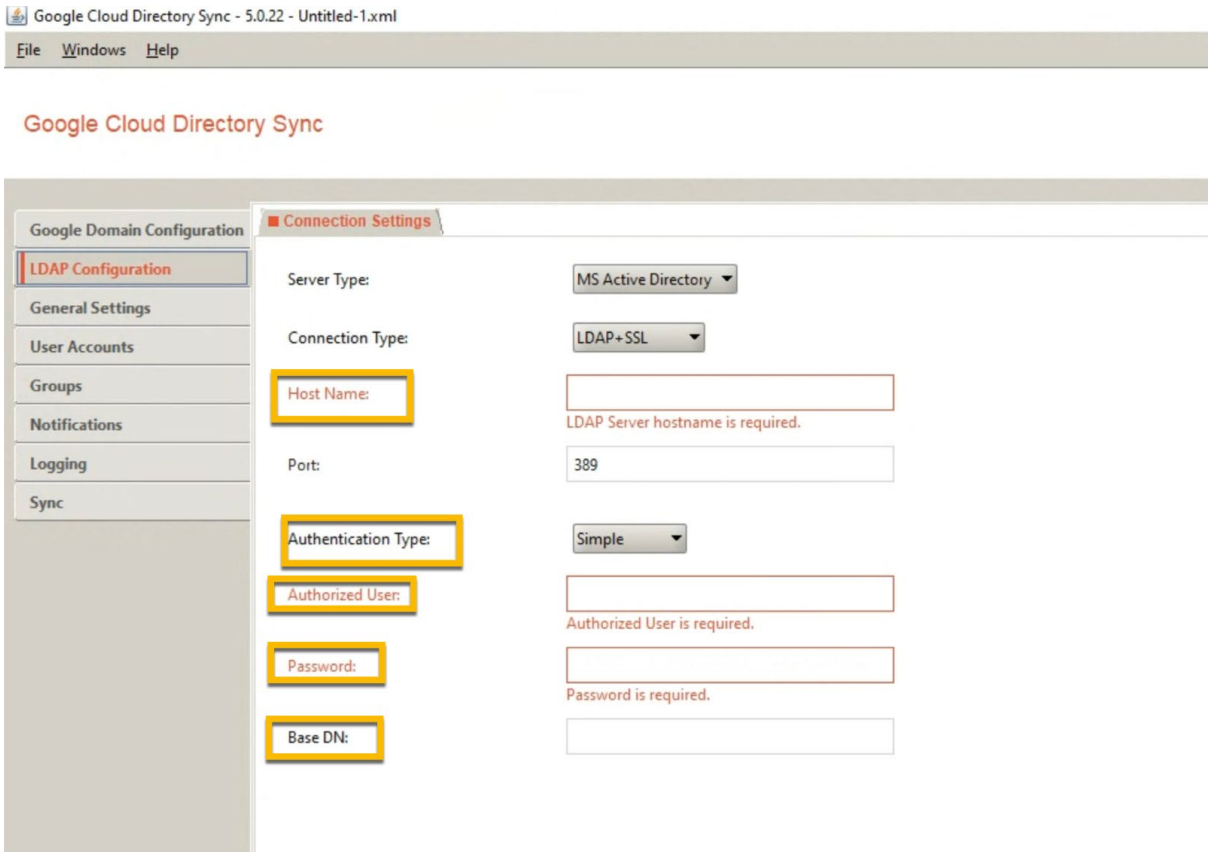


Figure 5.13 – LDAP configuration

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

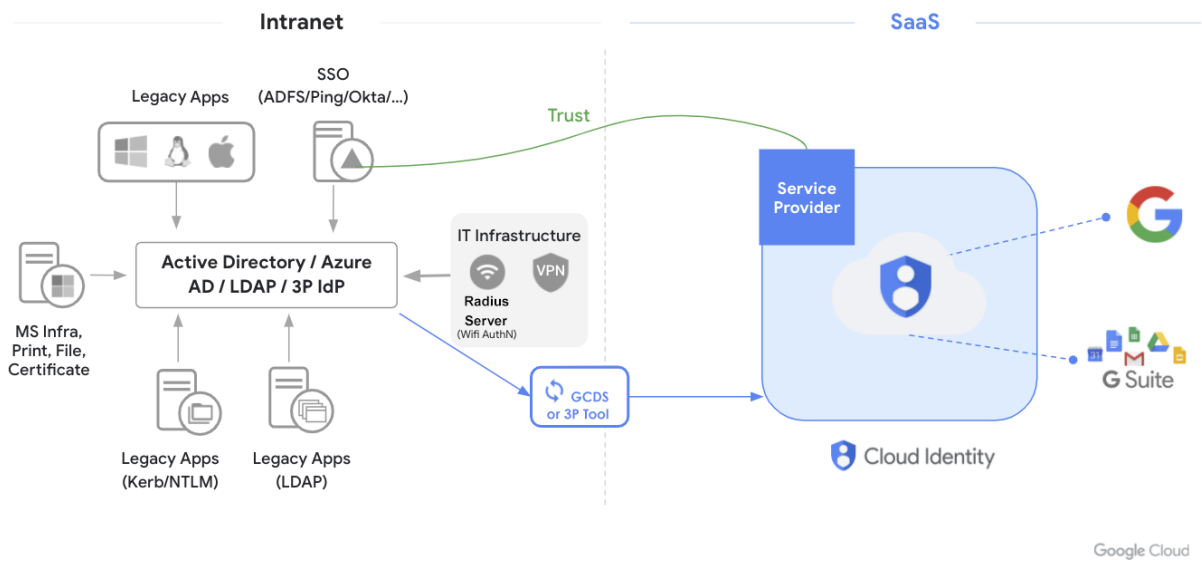


Figure 5.15 – Third party as an IdP

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

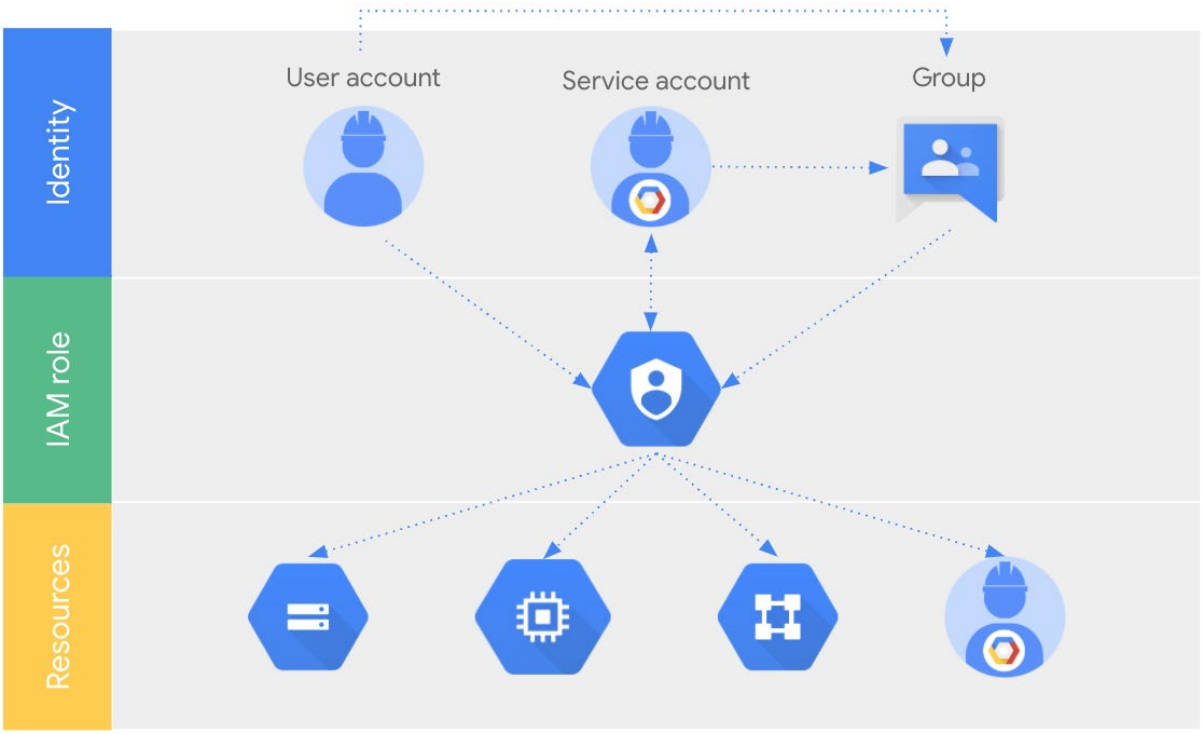


Figure 6.1 – IAM overview

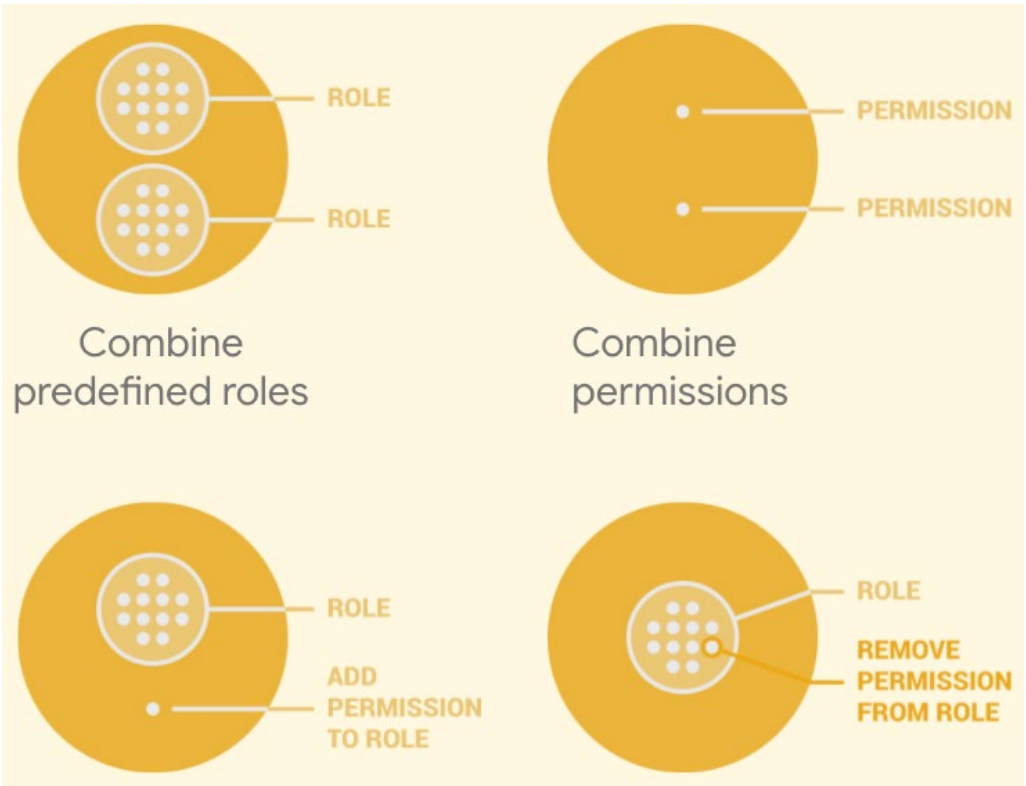


Figure 6.2 – IAM—custom roles

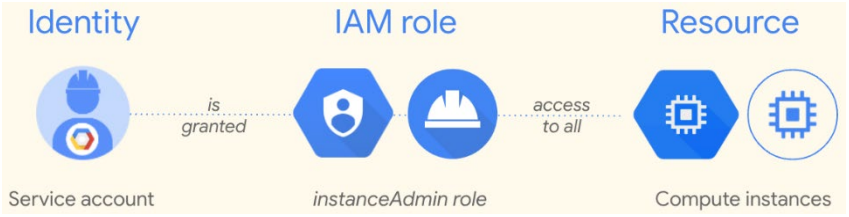


Figure 6.3 – Service account and resource

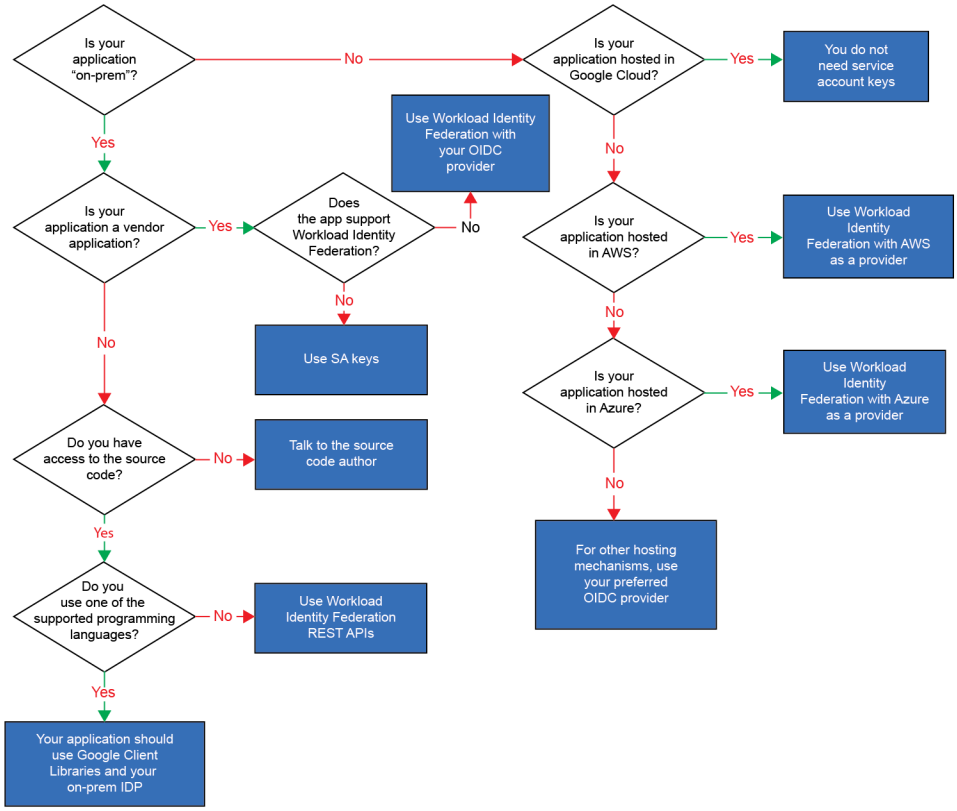


Figure 6.4 – Decision tree for service account keys

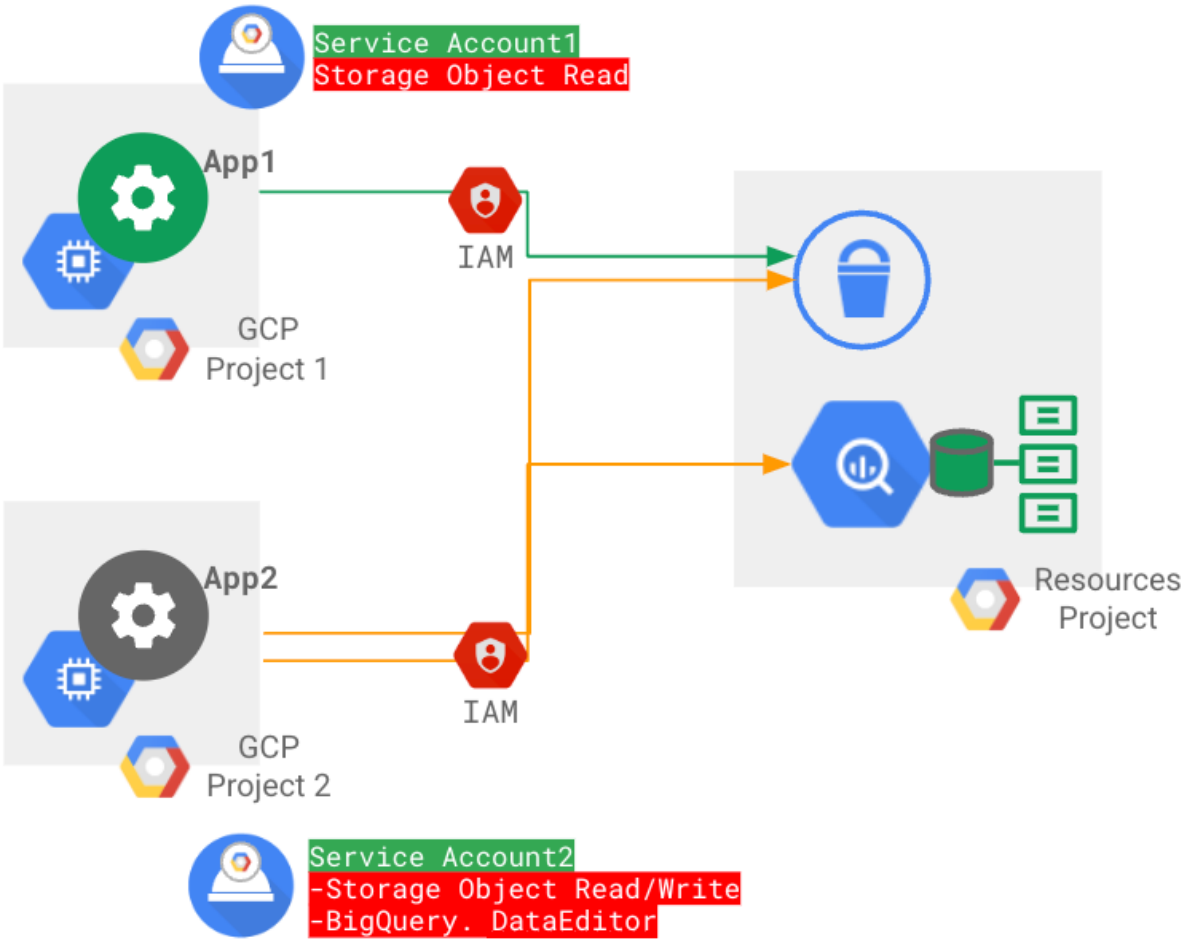


Figure 6.5 – Cross-project service account access

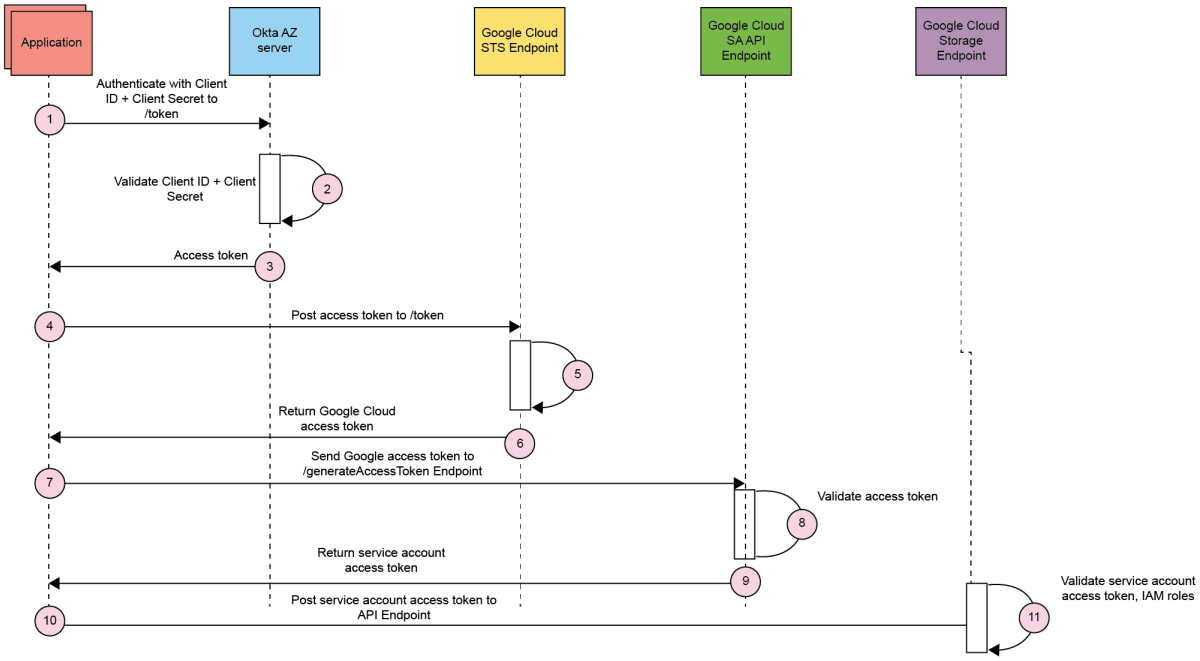


Figure 6.6 – Data flow for WIF with Okta

Chapter 7: Virtual Private Cloud

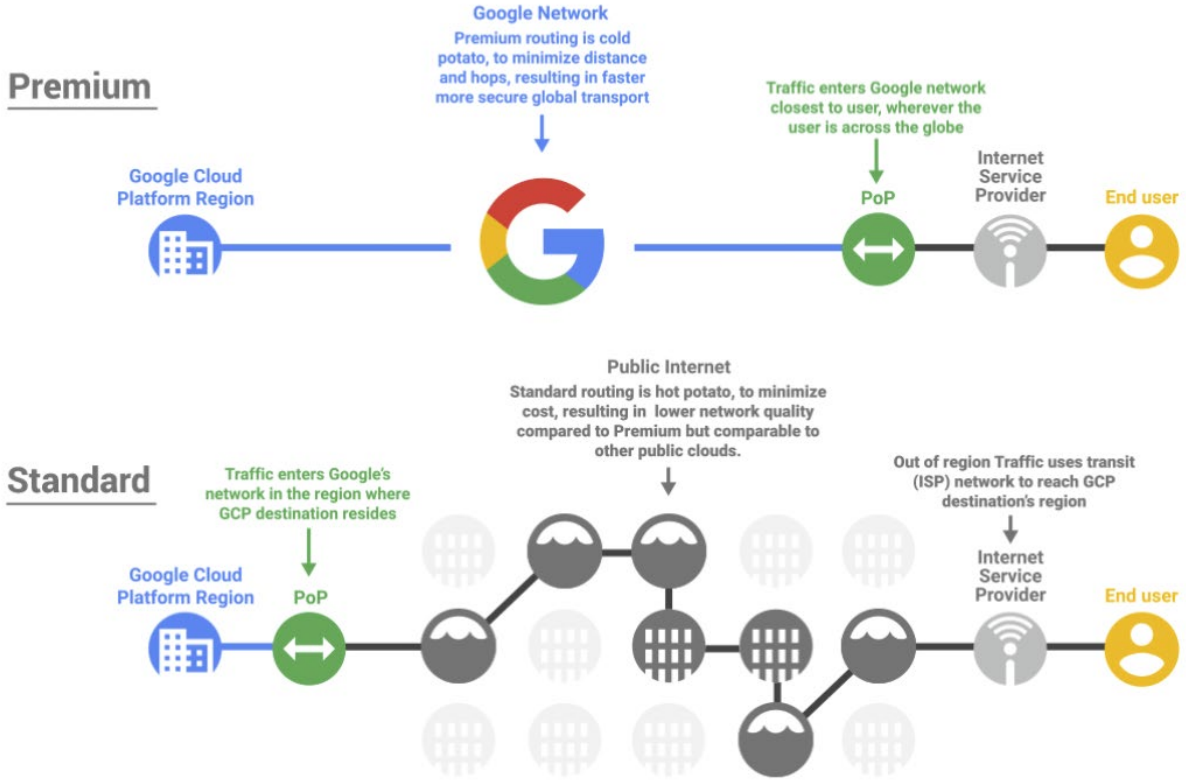
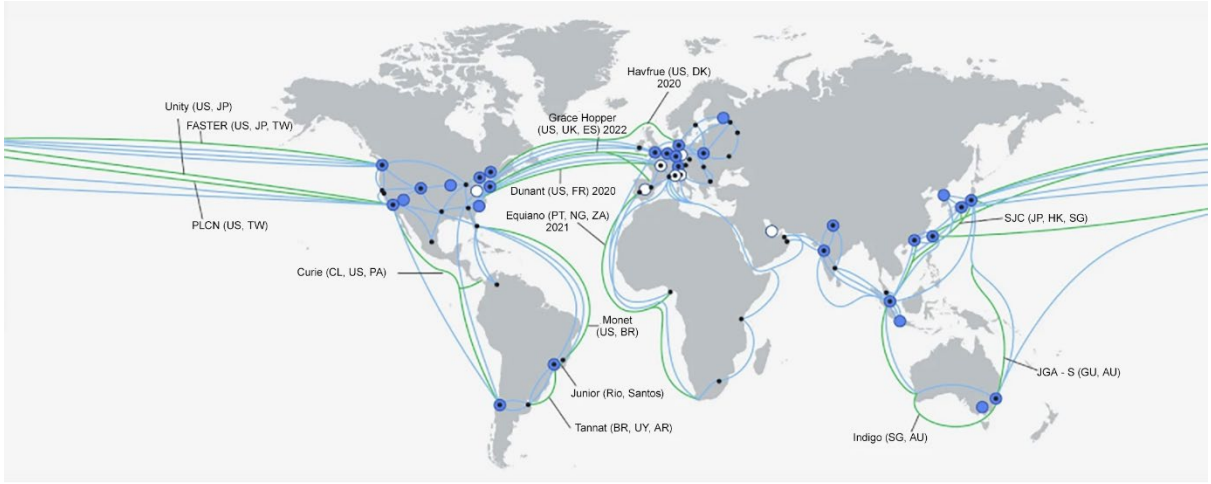


Figure 7.1 – Google Cloud network tiers



AVAILABLE IN

29 REGIONS

88 ZONES

146 NETWORK EDGE LOCATIONS

200+ COUNTRIES AND TERRITORIES

COMING SOON! Google Cloud will continue expanding into the following regions: Doha (Qatar), Paris (France), Milan (Italy), Madrid (Spain), Turin (Italy), Columbus (US), Berlin (Germany), Dammam (Kingdom of Saudi Arabia), Dallas (Texas), and Tel Aviv (Israel).

Figure 7.2 – Google Cloud region locations

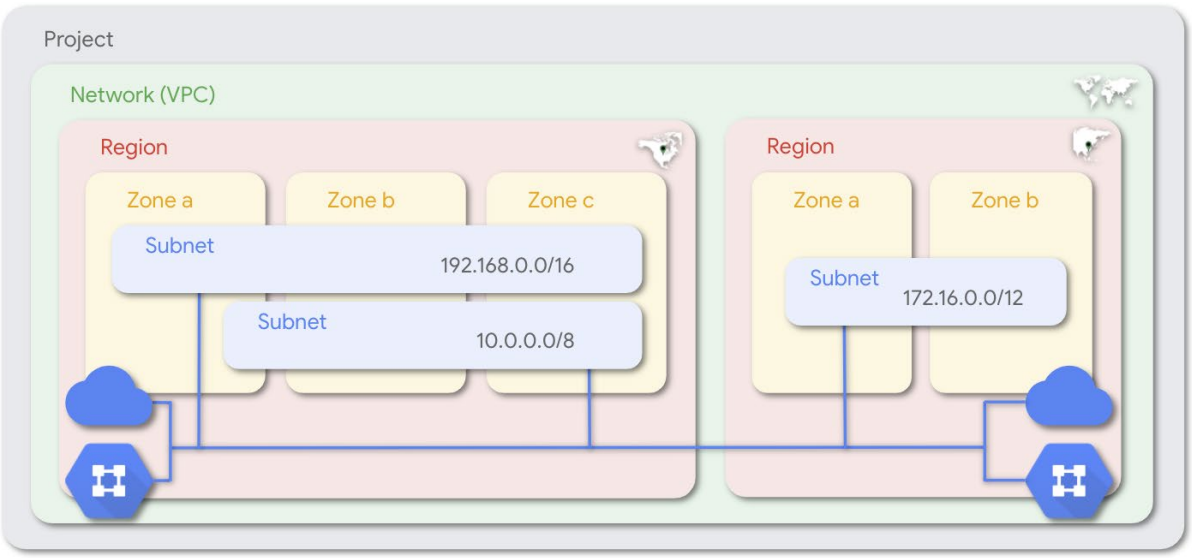


Figure 7.3 – Google network components

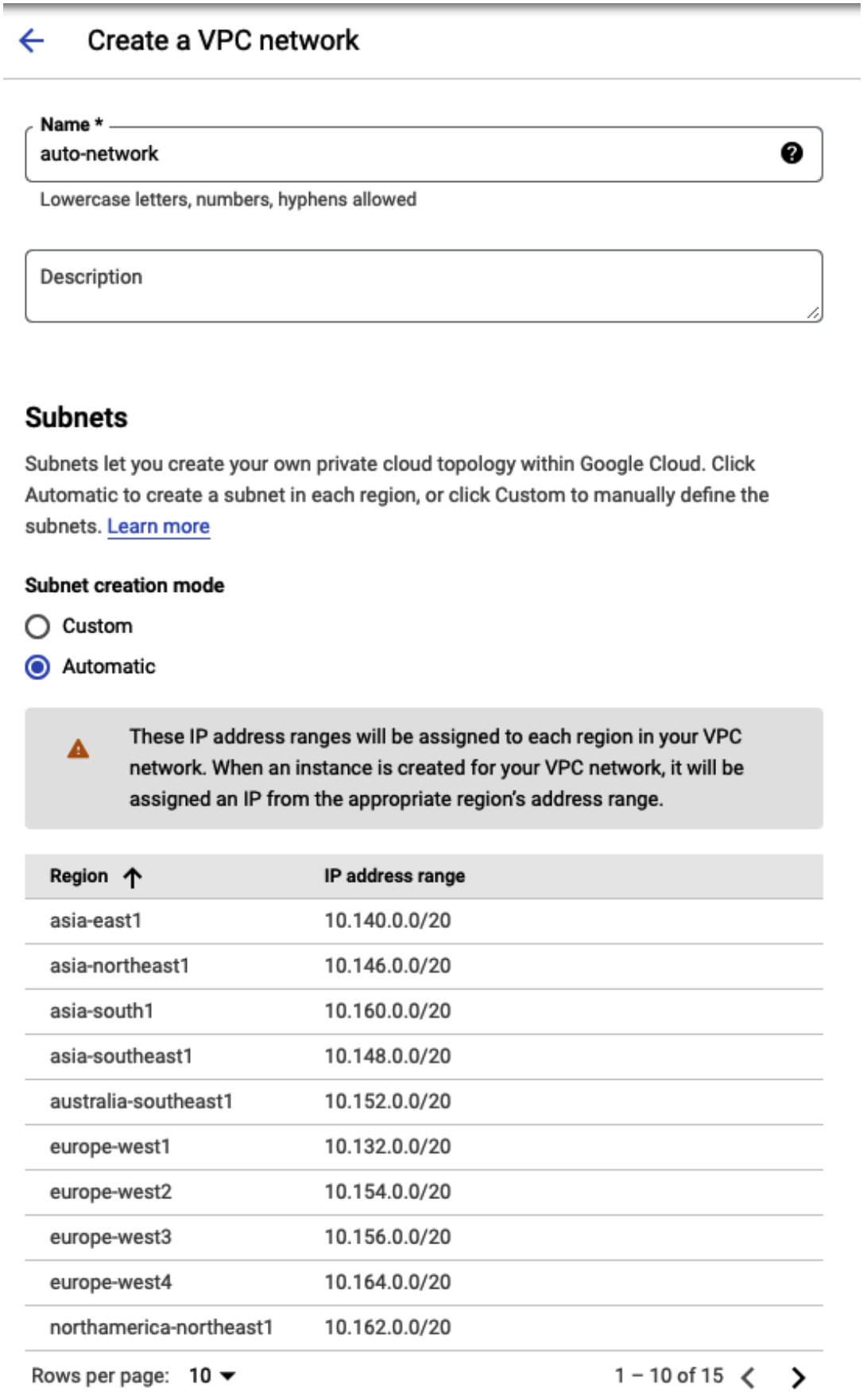


Figure 7.4 – VPC creation – auto mode

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

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	
auto-network-allow-custom	Ingress	Apply to all	IP ranges: 10.128.0.0/9	all	Allow	65,534	EDIT
auto-network-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65,534	
auto-network-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65,534	
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

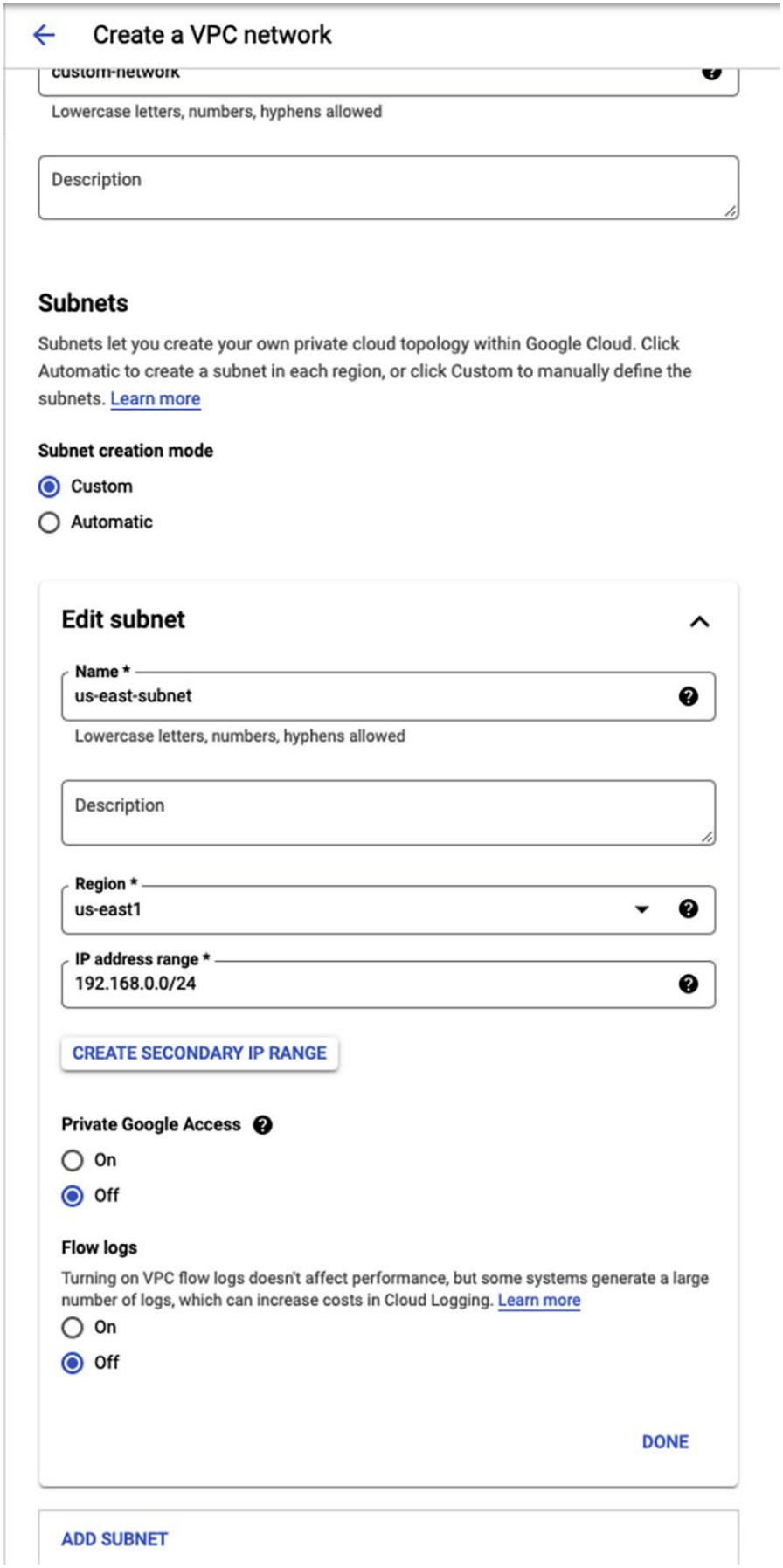


Figure 7.6 – Custom VPC creation

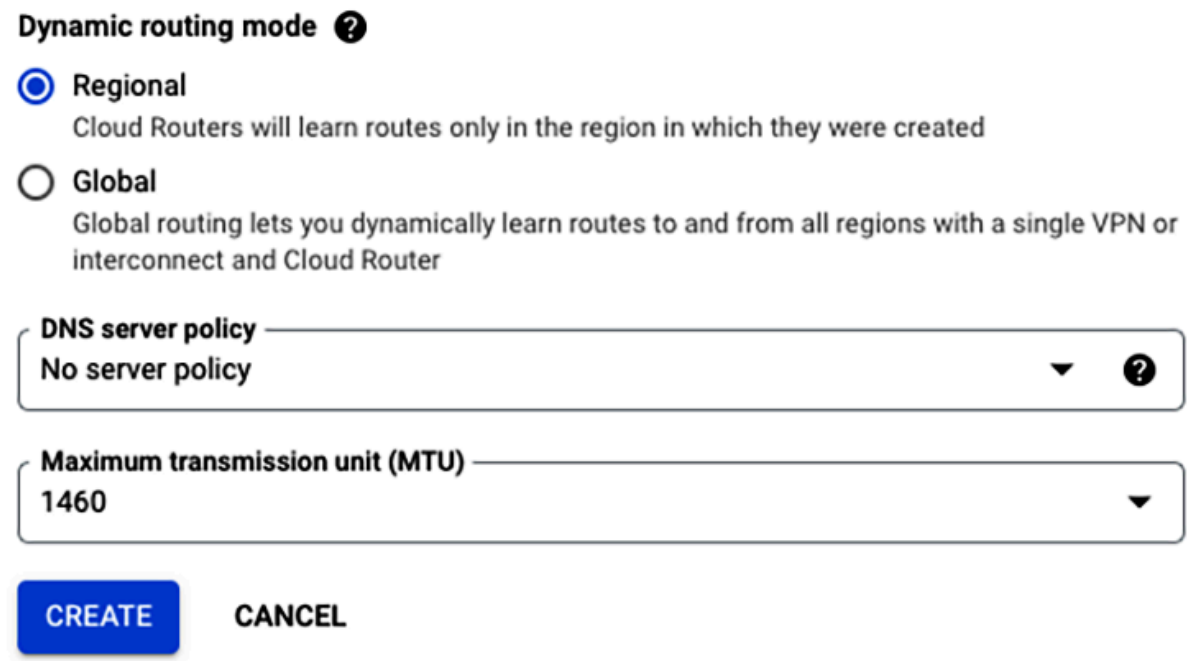


Figure 7.7 – Dynamic routing

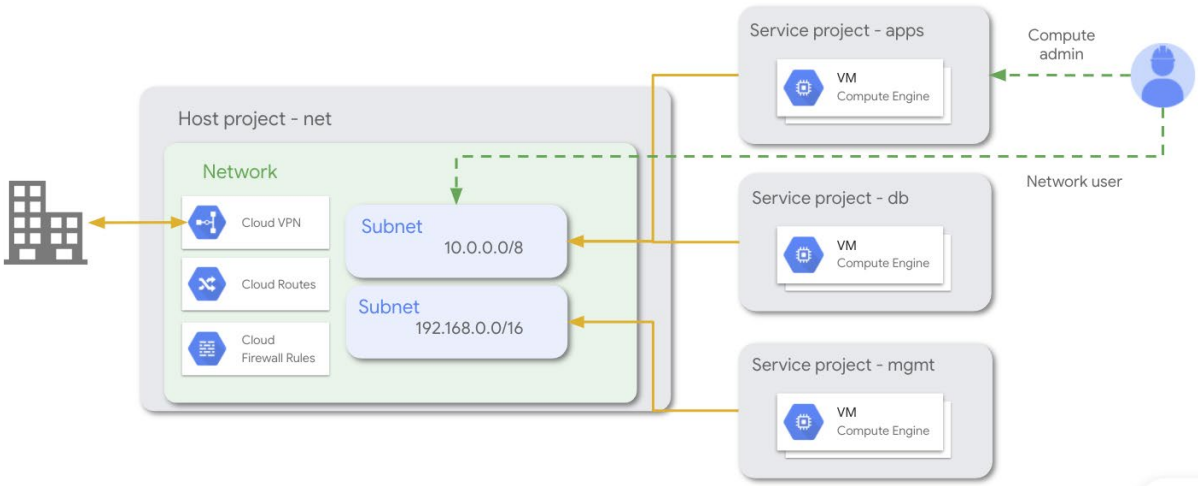


Figure 7.8 – Shared VPC network

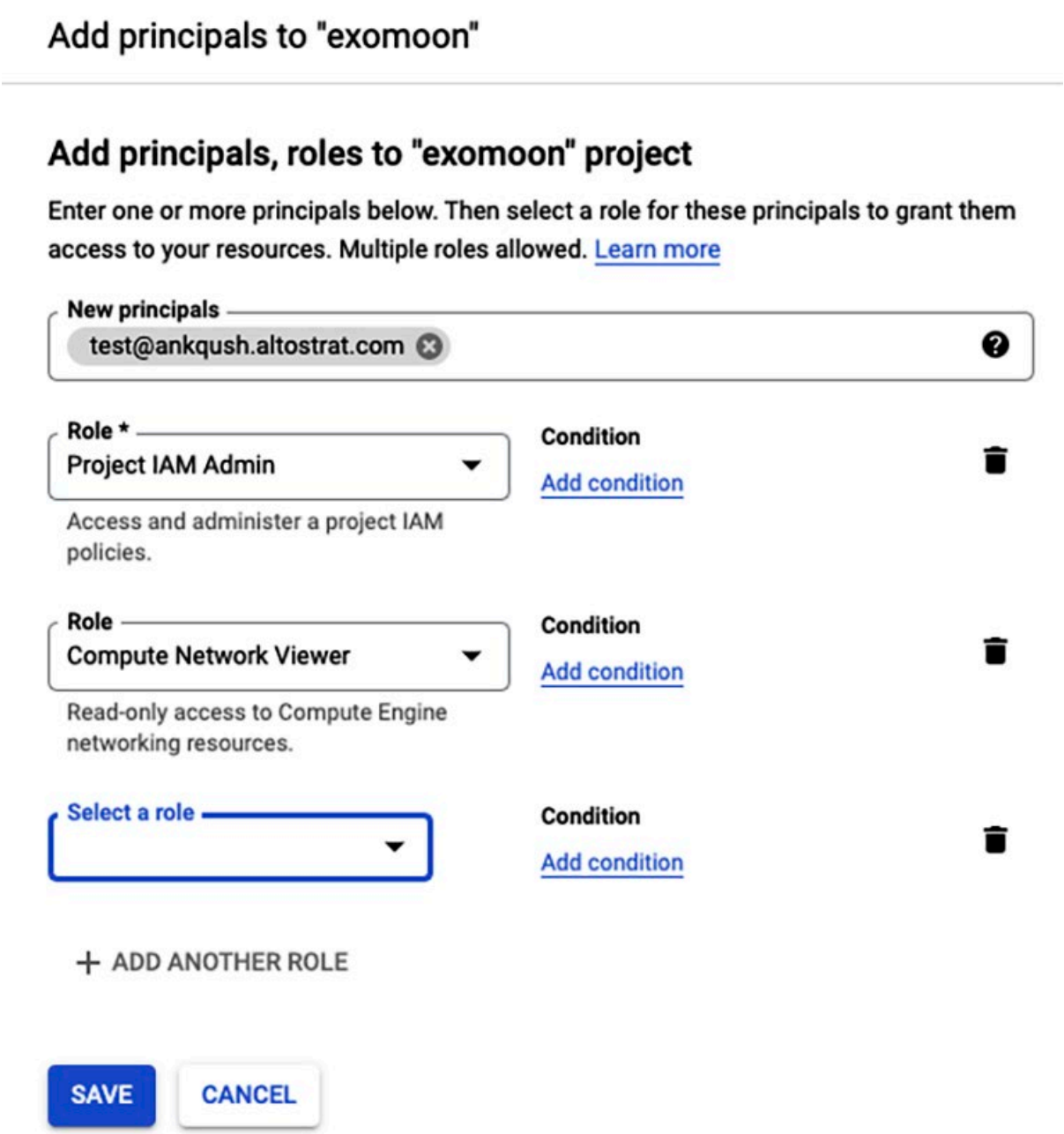


Figure 7.9 – Assign IAM roles for Shared VPC

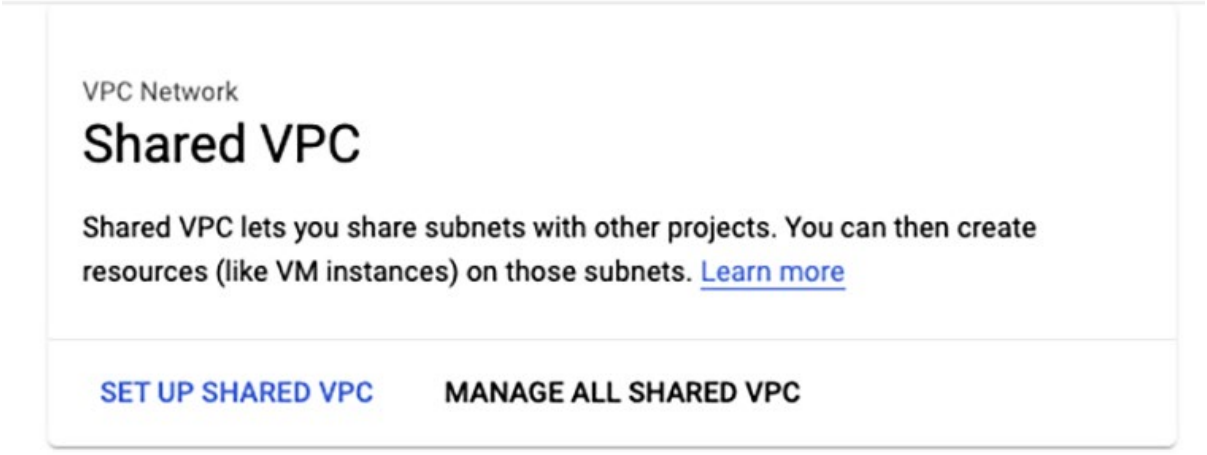


Figure 7.10 – SET UP SHARED VPC

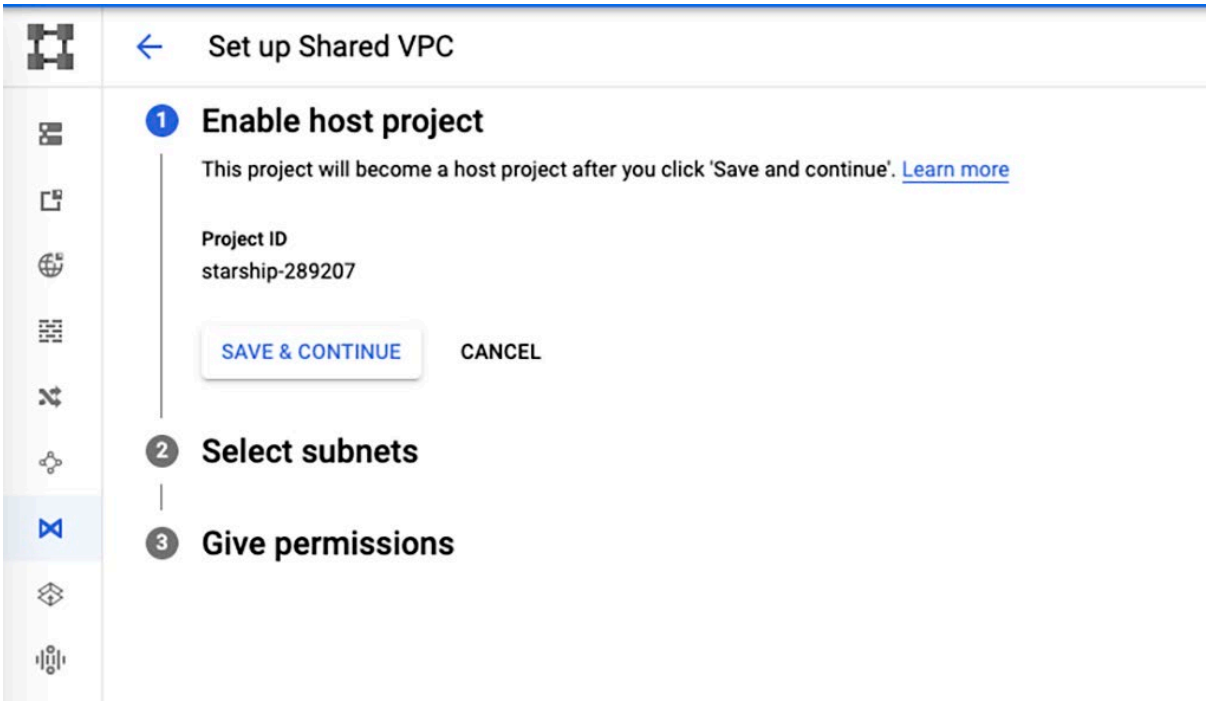


Figure 7.11 – Enable host project

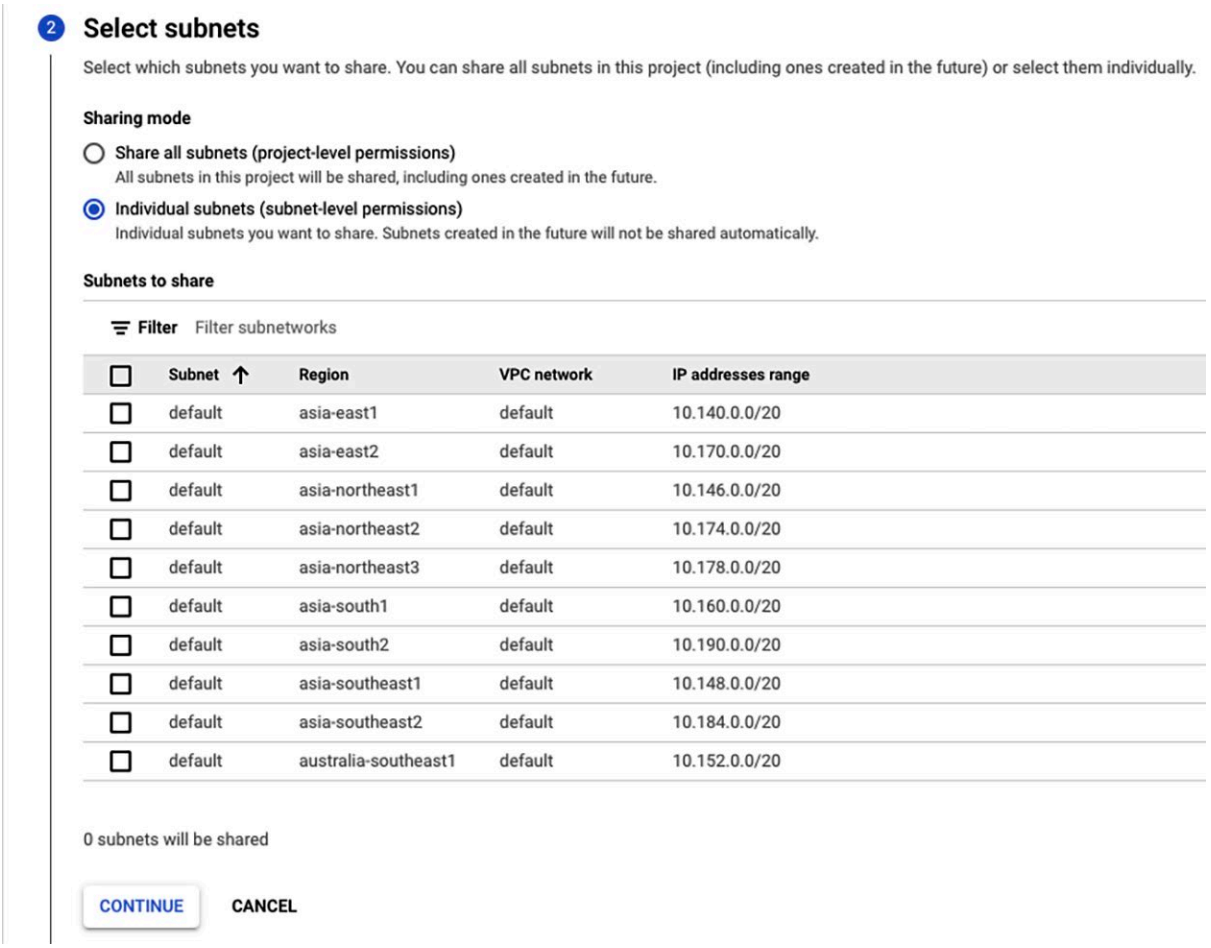


Figure 7.12 – Select subnets

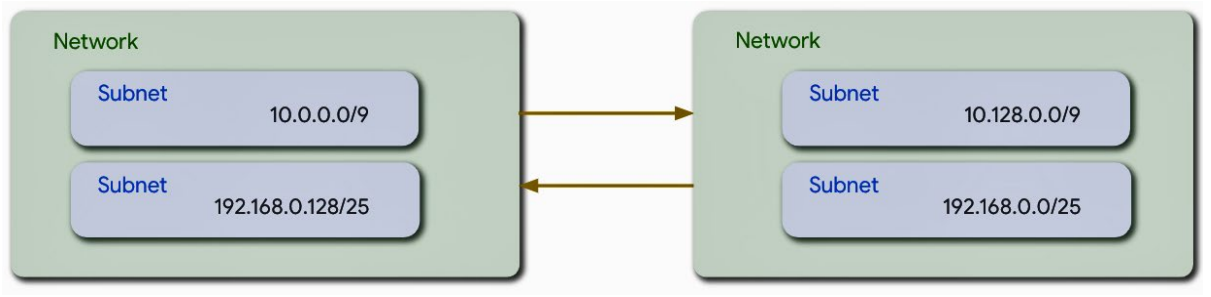


Figure 7.13 – VPC peering

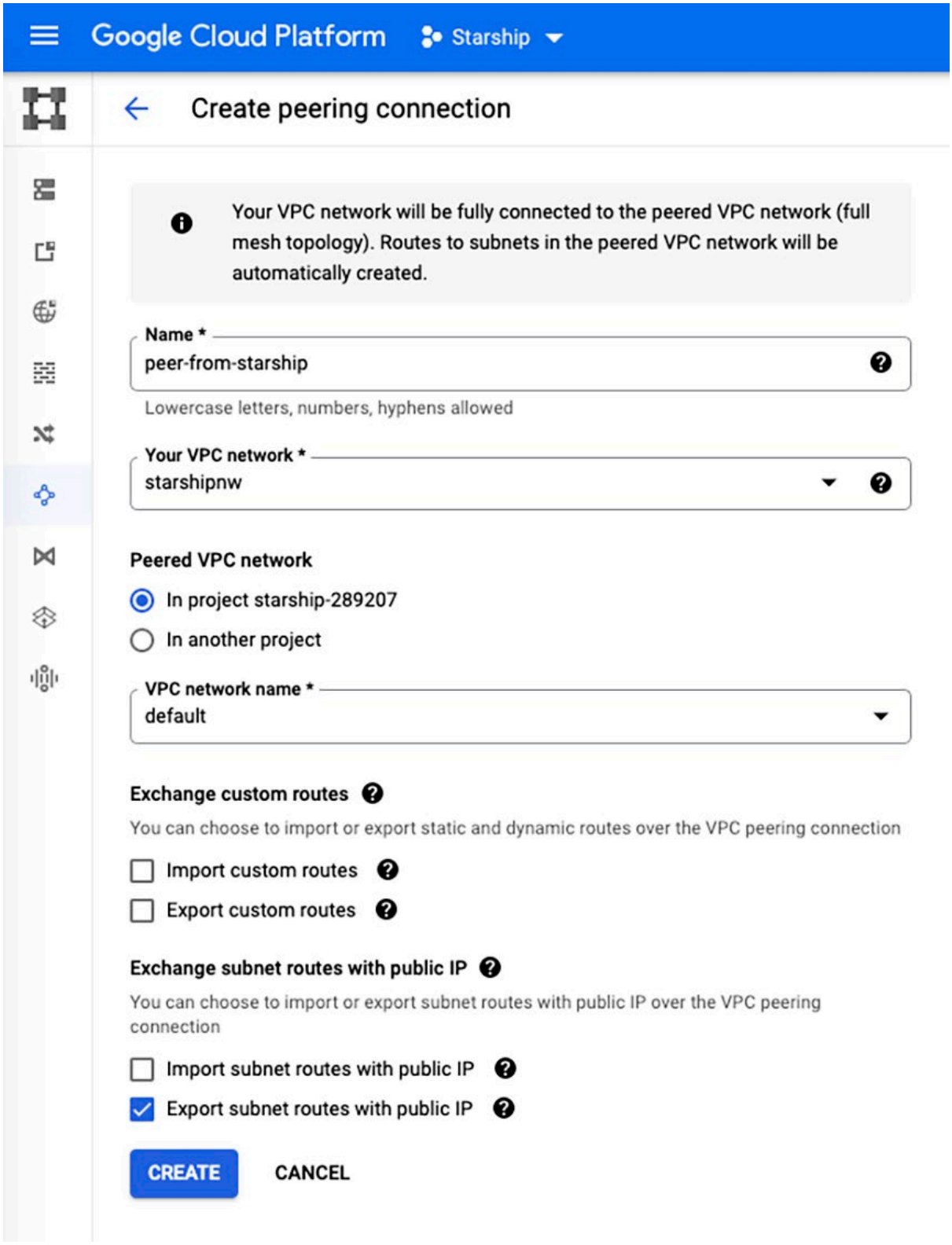


Figure 7.14 – Create peering connection

	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 billed 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

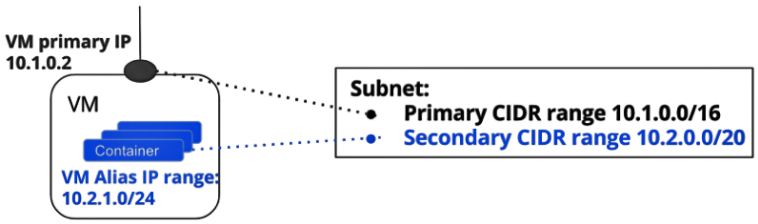


Figure 7.16 – Subnet CIDR ranges

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

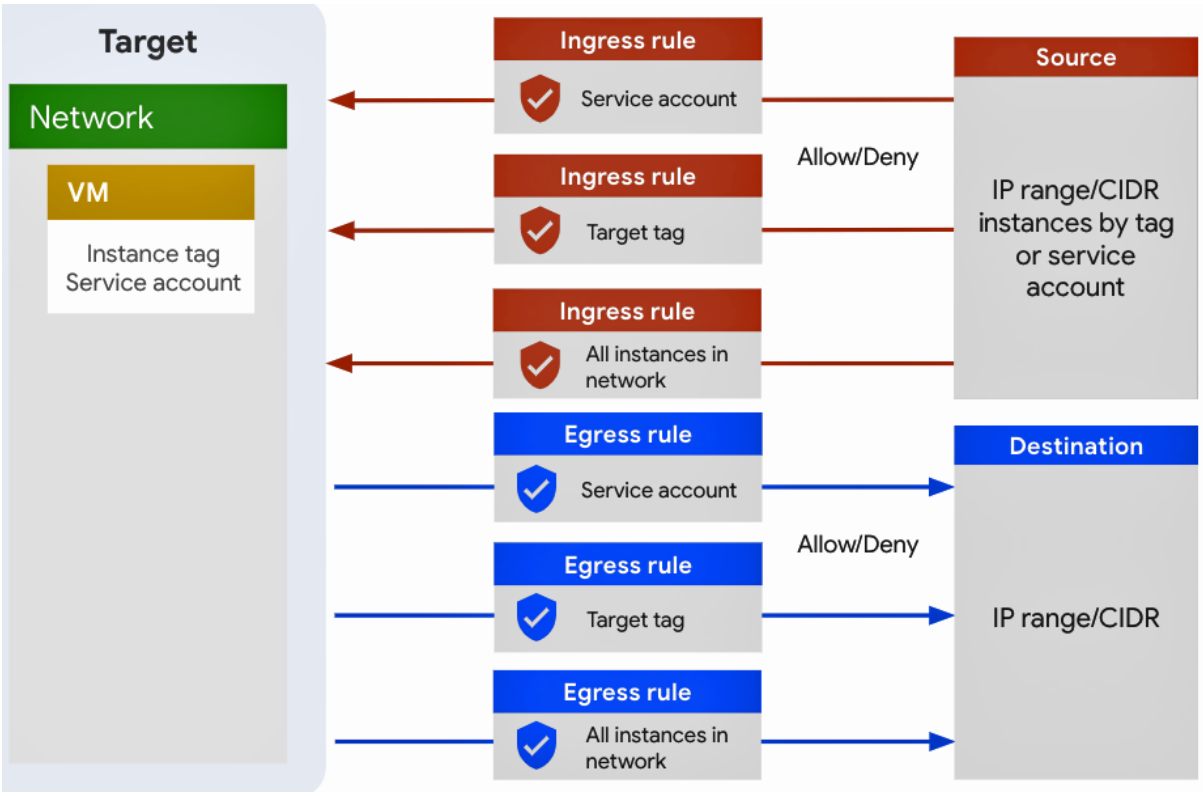


Figure 7.18 – VPC firewall rules

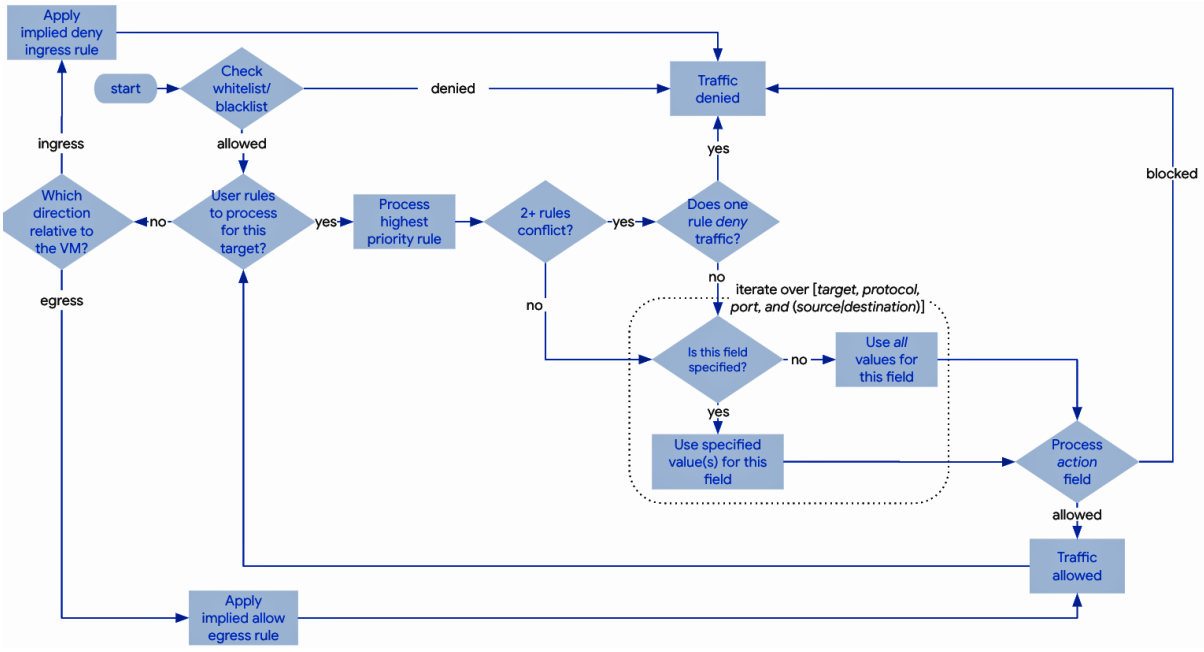


Figure 7.19 – Firewall rule evaluation logic

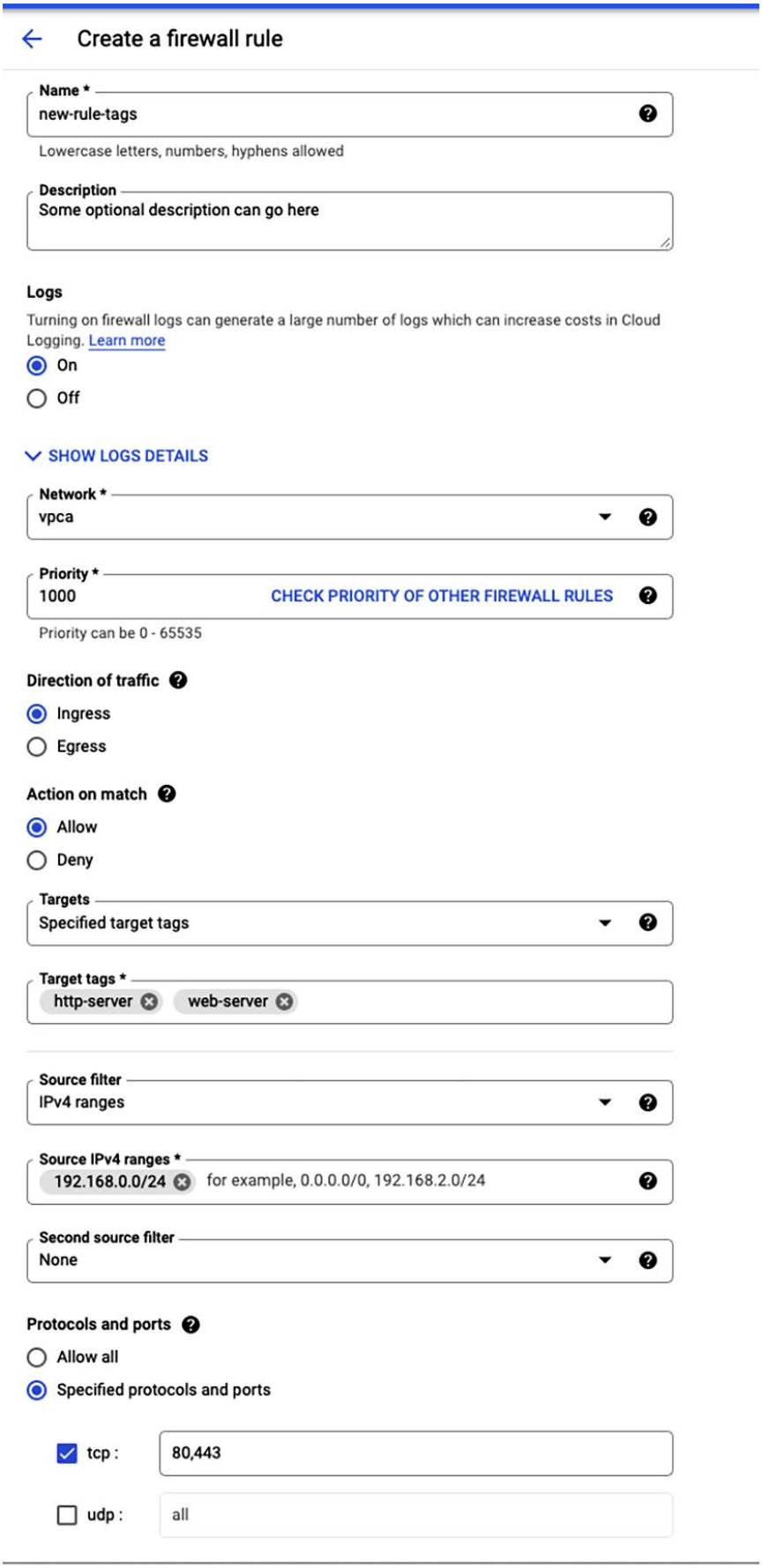


Figure 7.20 – Create a firewall rule using target tags

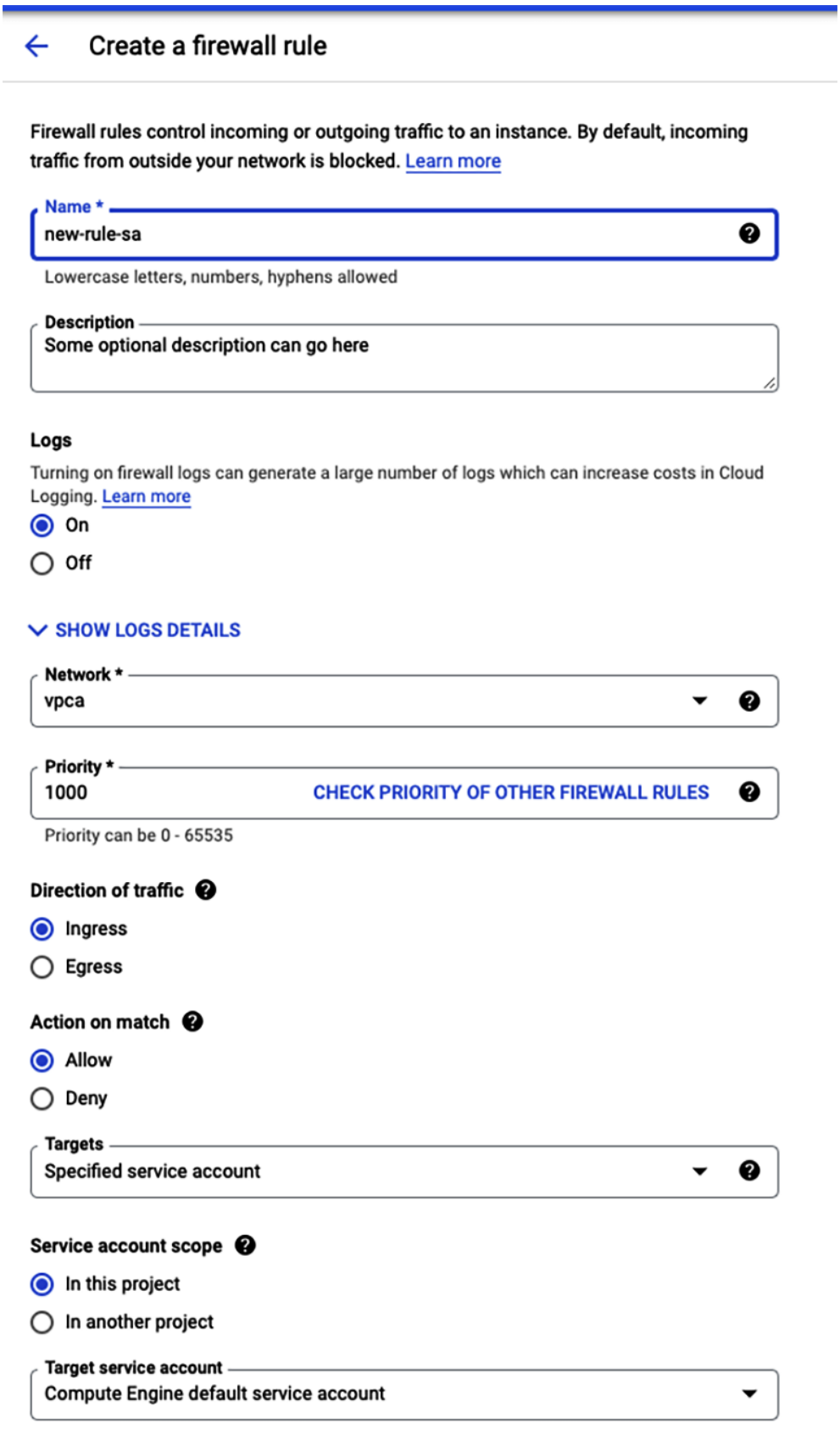


Figure 7.21 – Create a firewall rule using the service account

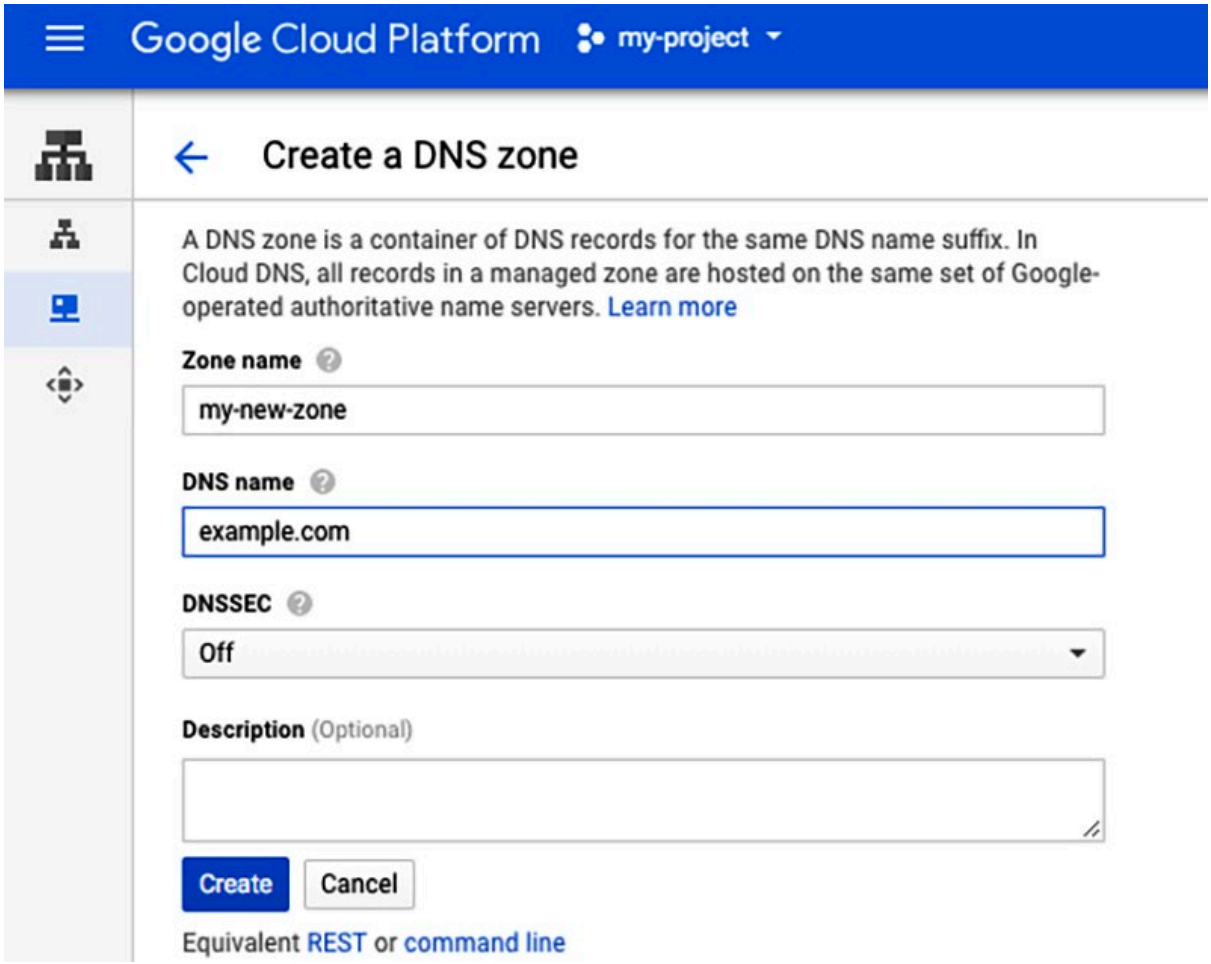


Figure 7.22 – Create a DNS zone

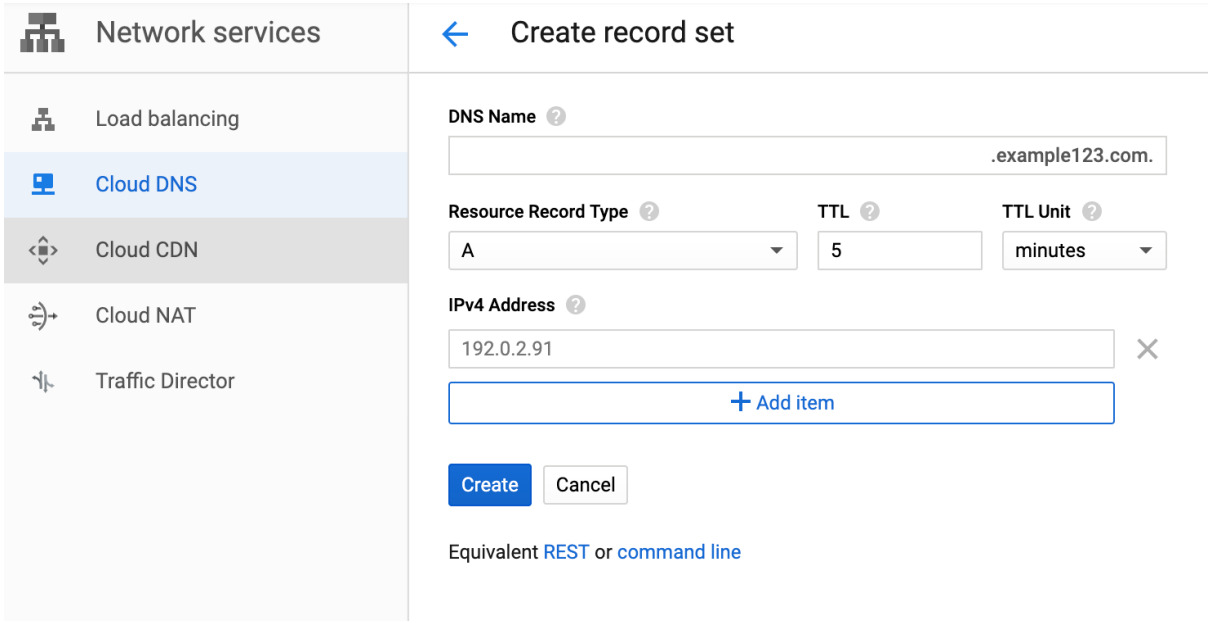


Figure 7.23 – Create a record sets

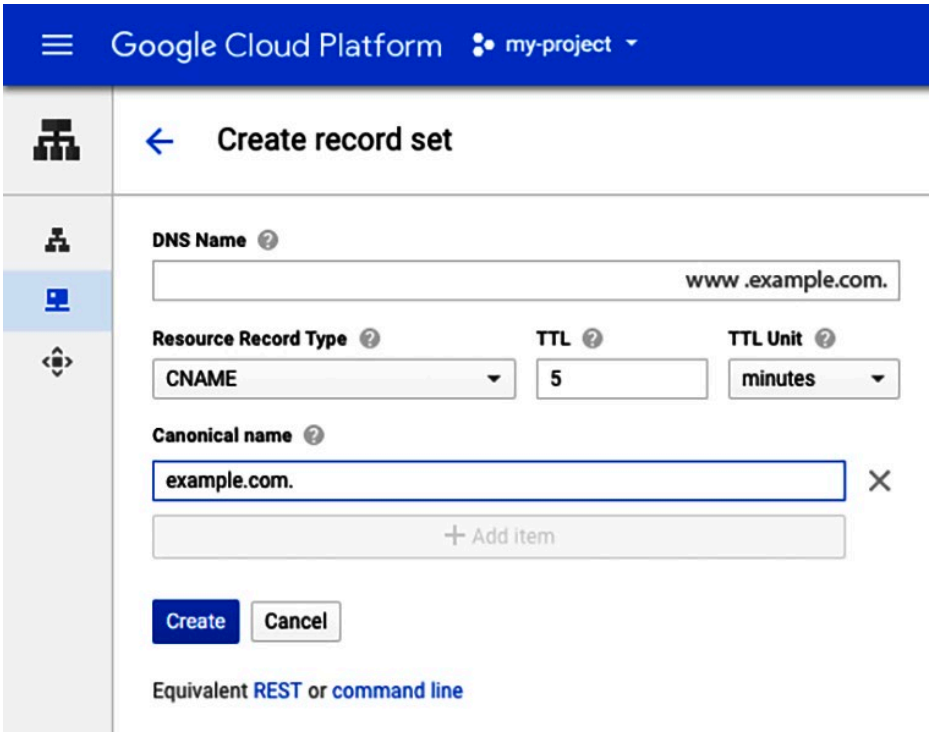


Figure 7.24 – Create a CNAME record

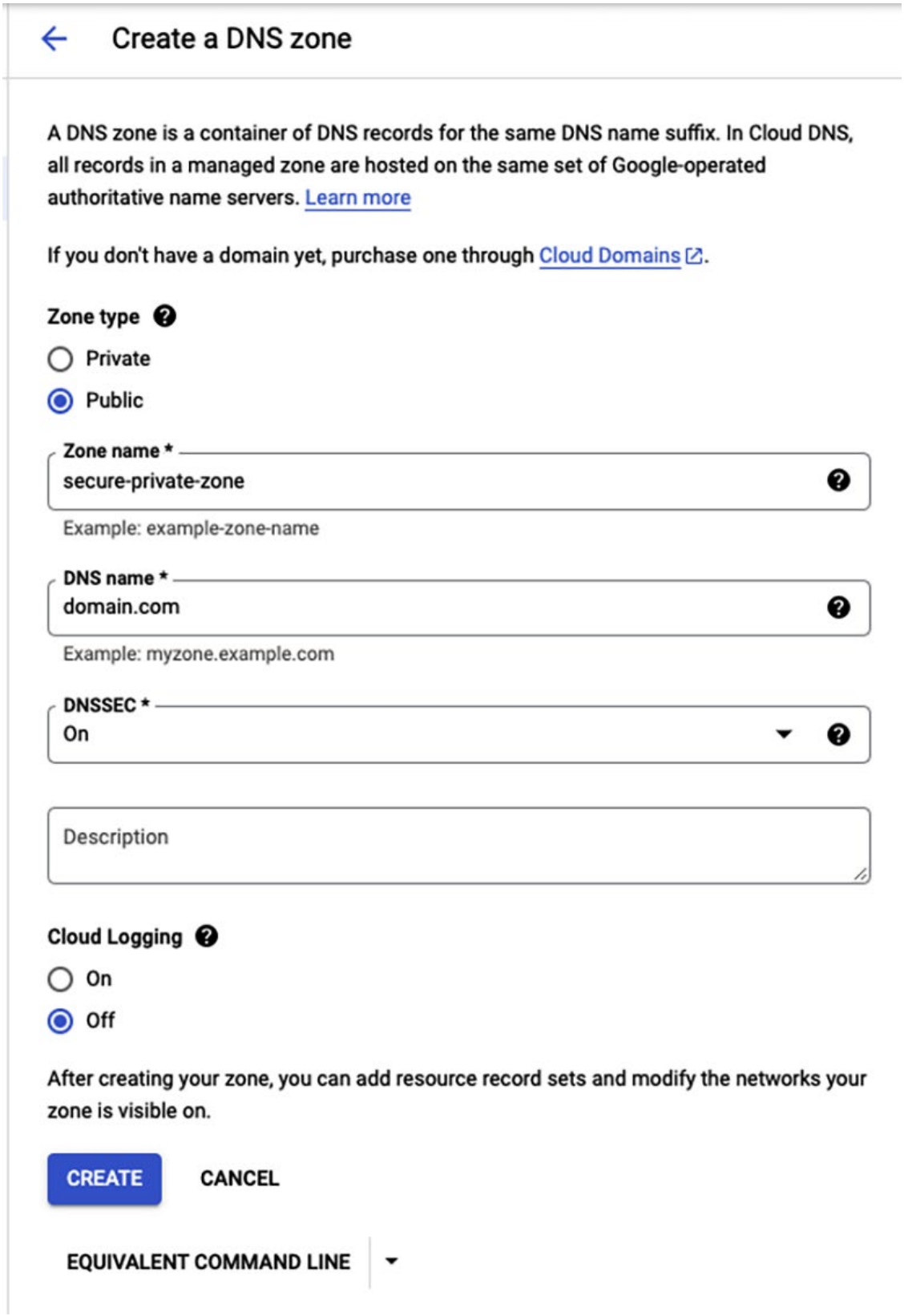
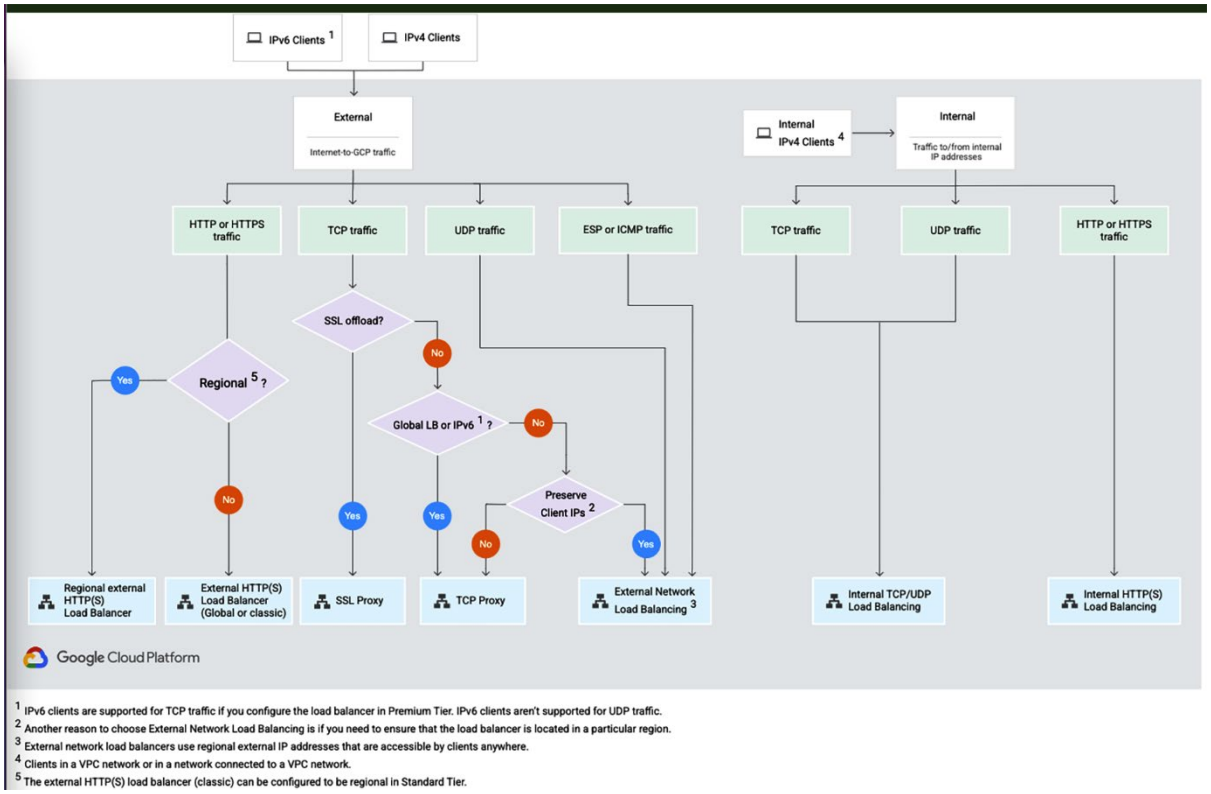


Figure 7.25 – Enable DNSSEC for a private DNS zone

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

Figure 7.26 – Different types of Google Cloud load balancers



1 IPv6 clients are supported for TCP traffic if you configure the load balancer in Premium Tier. IPv6 clients aren't supported for UDP traffic.
2 Another reason to choose External Network Load Balancing is if you need to ensure that the load balancer is located in a particular region.
3 External network load balancers use regional external IP addresses that are accessible by clients anywhere.
4 Clients in a VPC network or in a network connected to a VPC network.
5 The external HTTP(S) load balancer (classic) can be configured to be regional in Standard Tier.

Figure 7.27 – Decision tree for choosing a load balancer

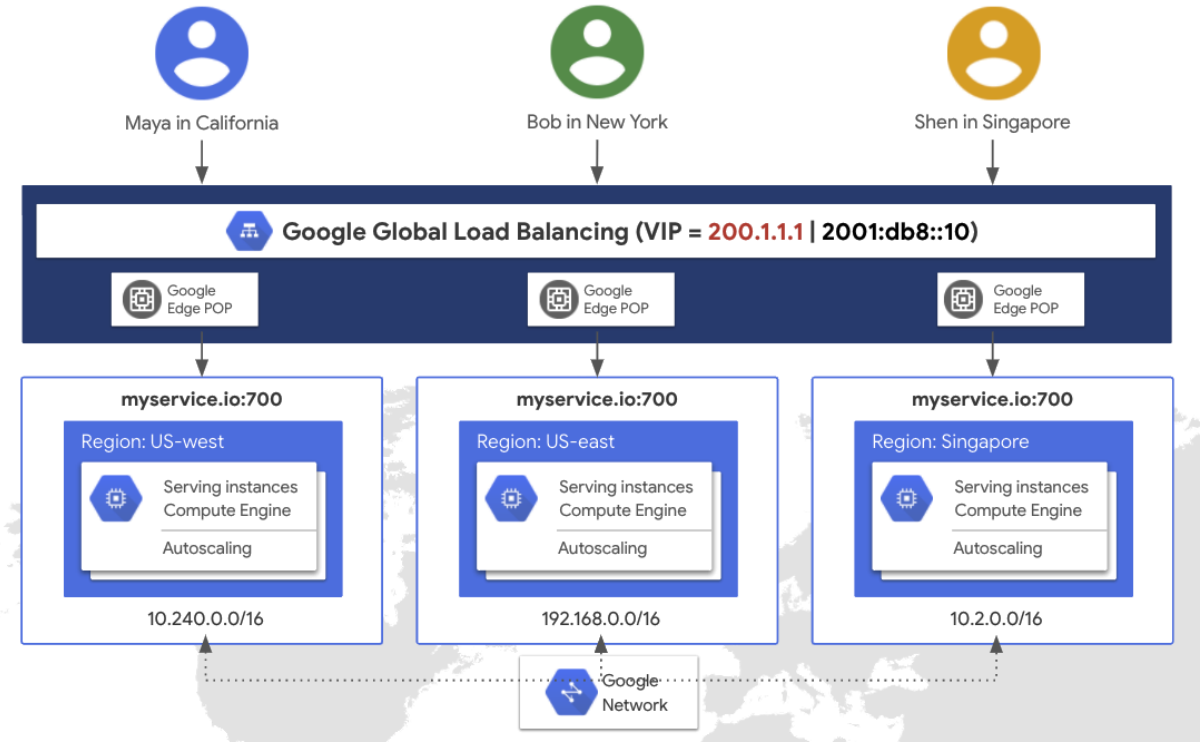


Figure 7.28 – External global HTTP(S) load balancing

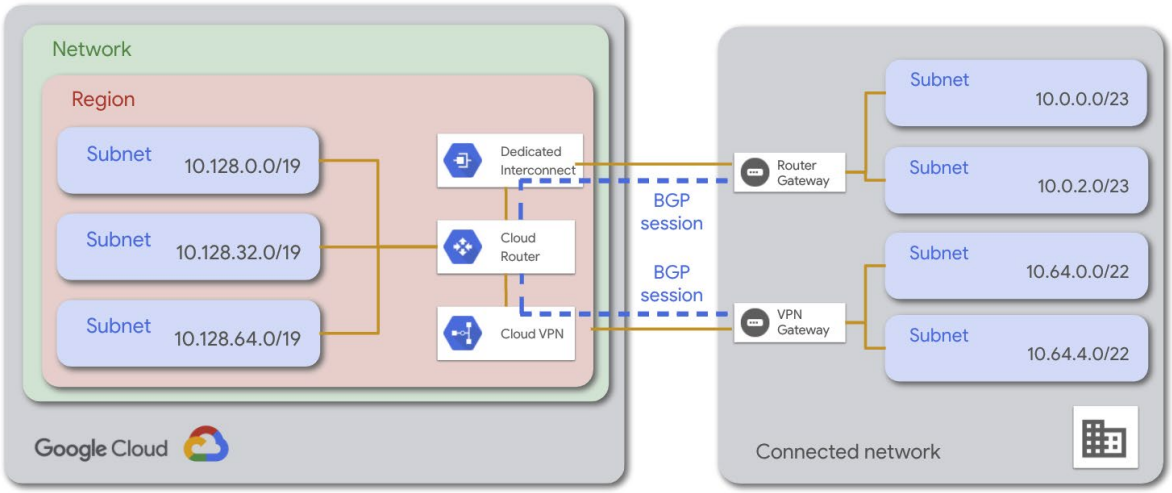


Figure 7.29 – Cloud Router

s

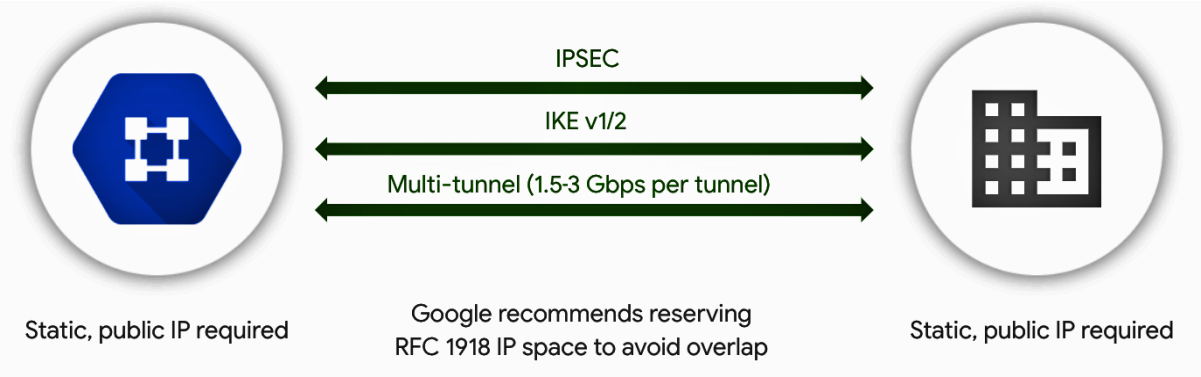


Figure 7.30 – Cloud VPN

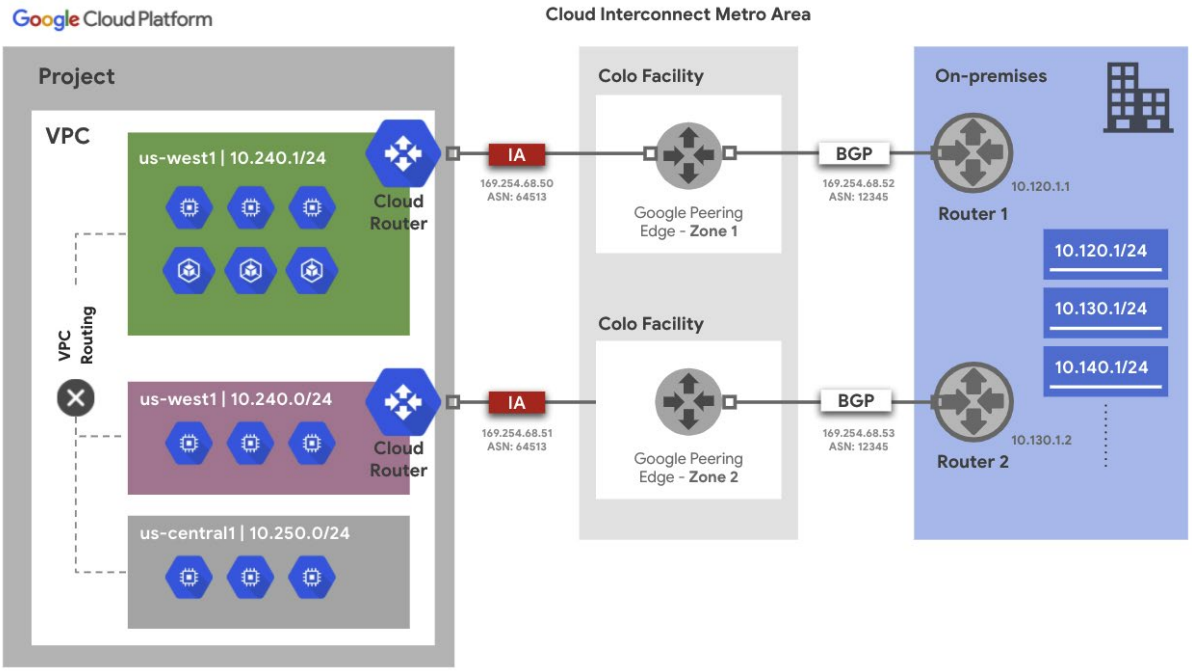


Figure 7.31 – Cloud Interconnect

Chapter 8: Advanced Network Security

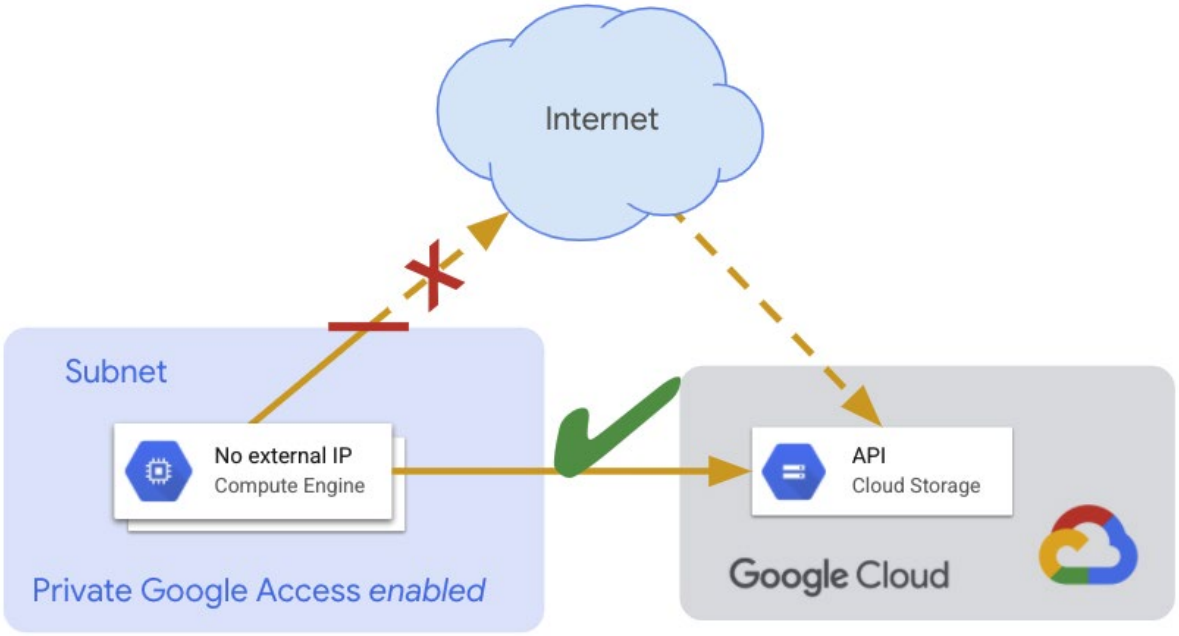


Figure 8.1 – Private Google Access

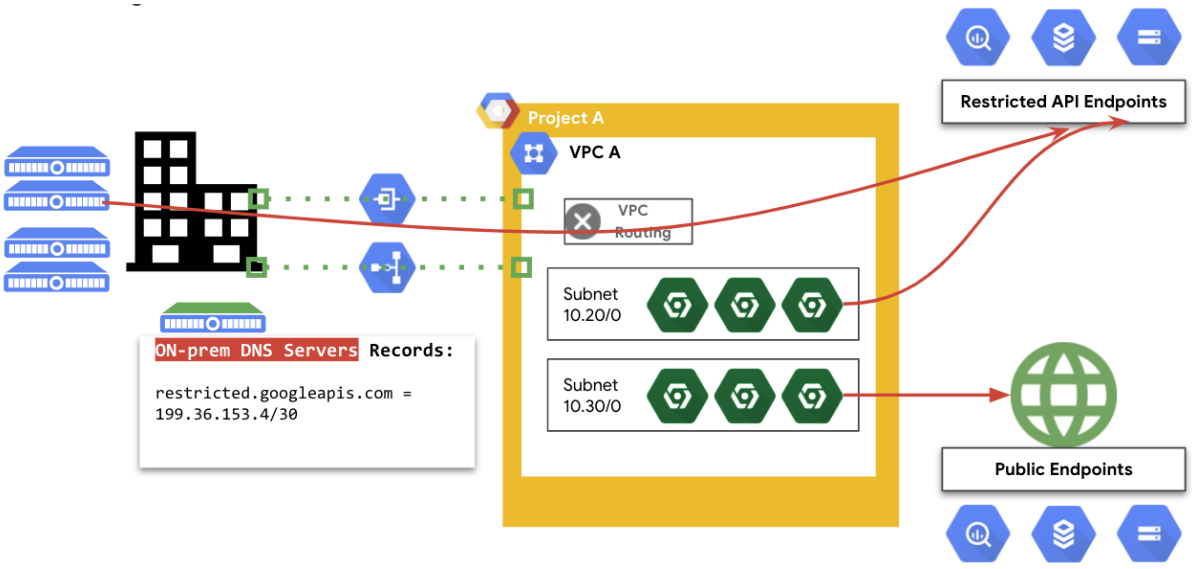


Figure 8.2 – Private Google Access for on-premises services

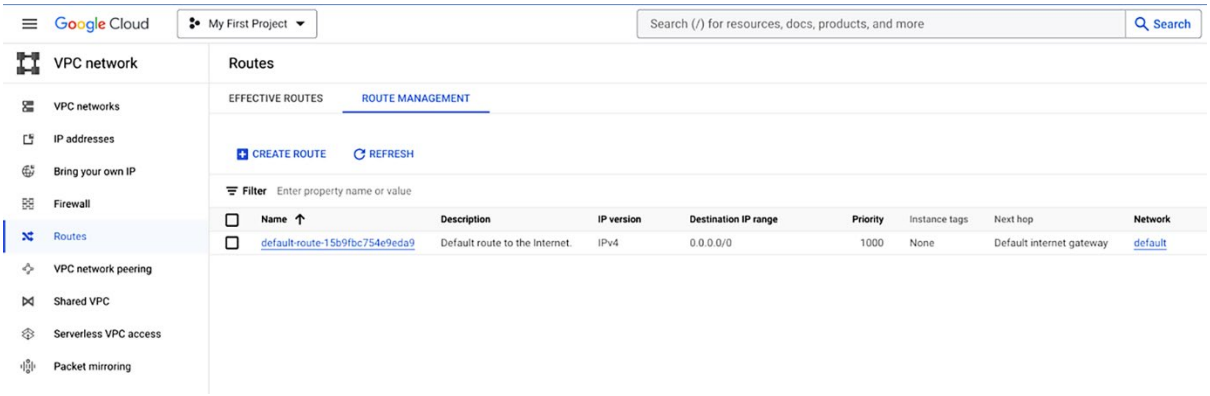


Figure 8.3 – Default internet gateway route

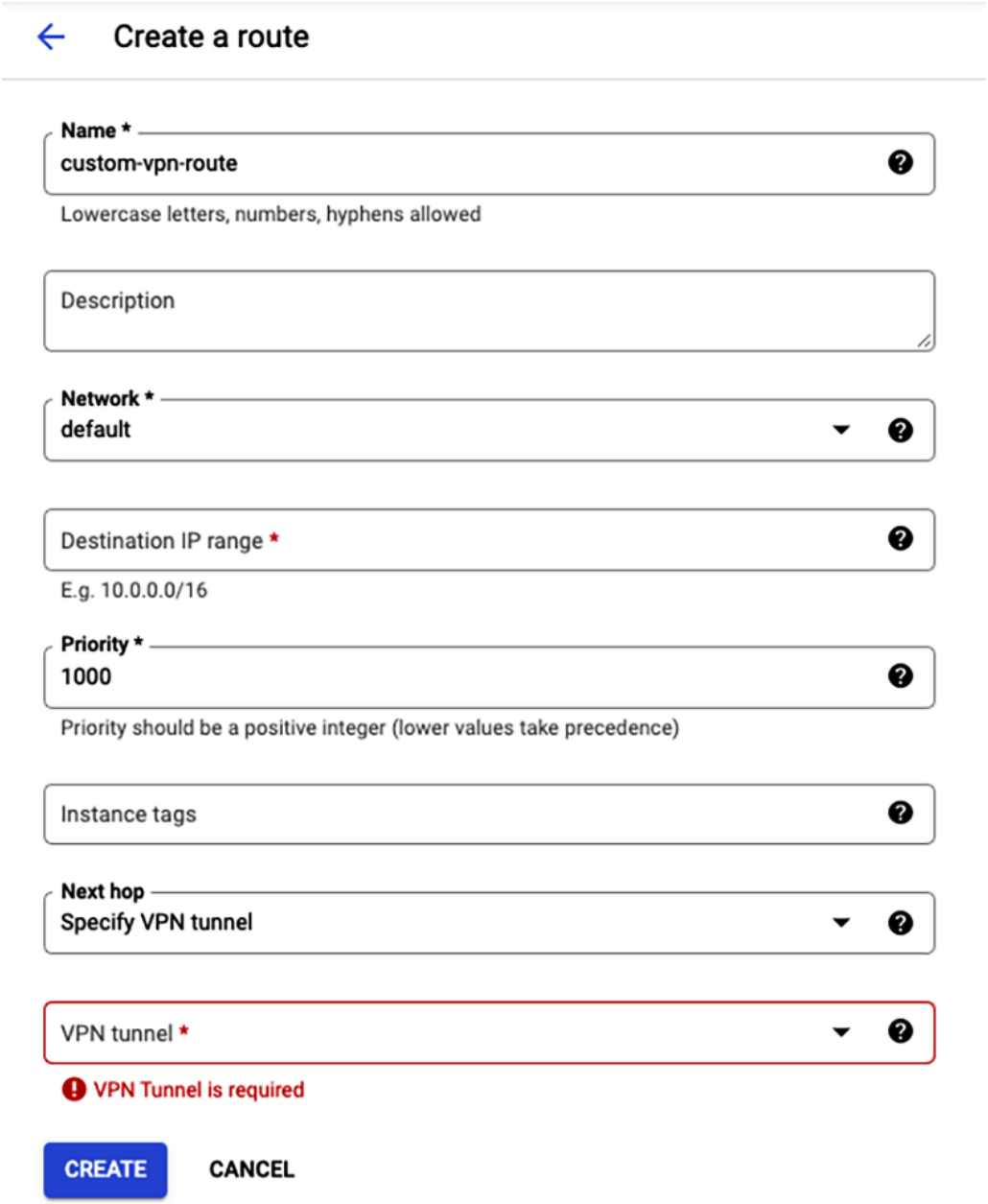


Figure 8.4 – Create a route for the VPN tunnel

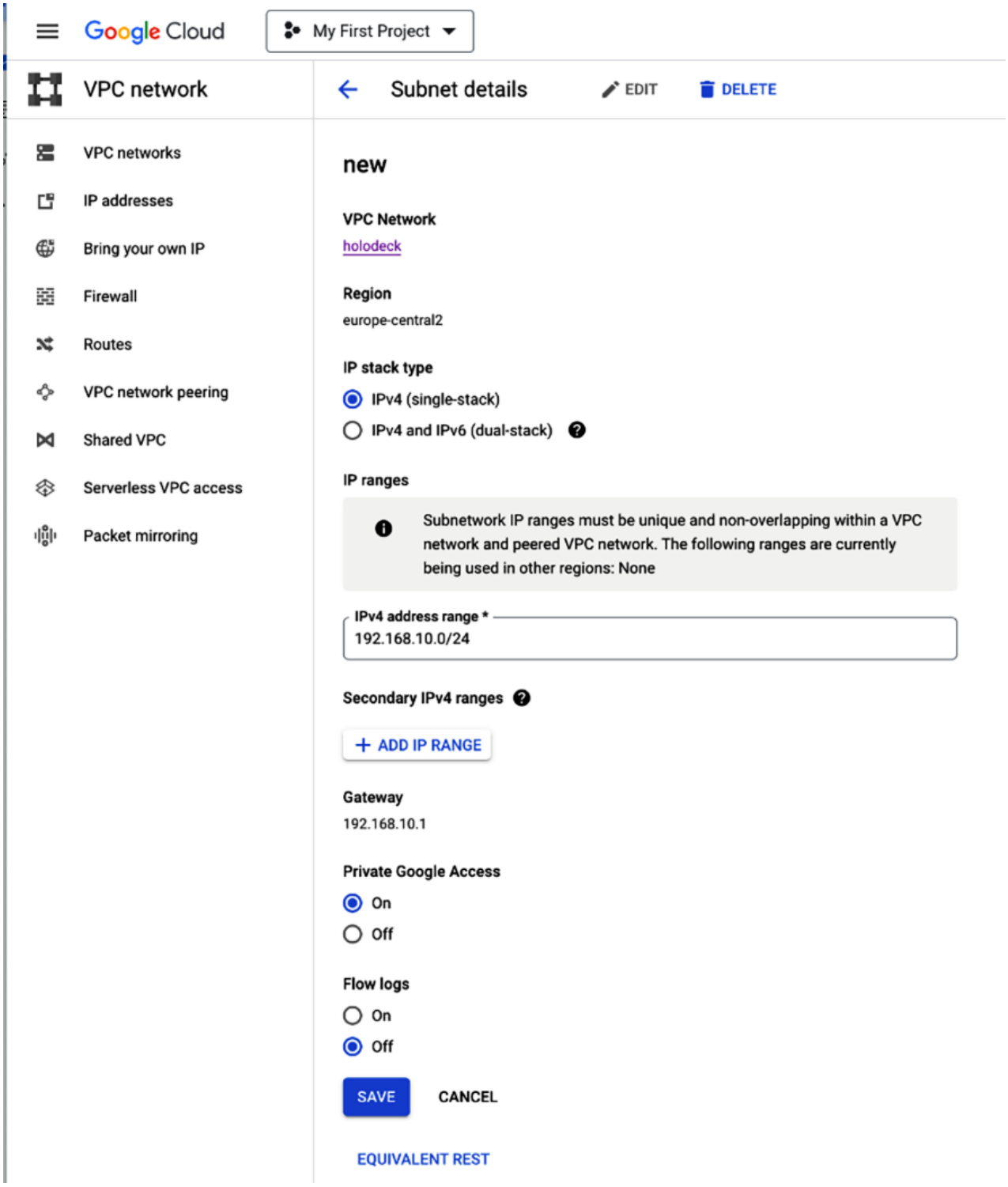


Figure 8.5 – Enable Private Google Access for the subnet

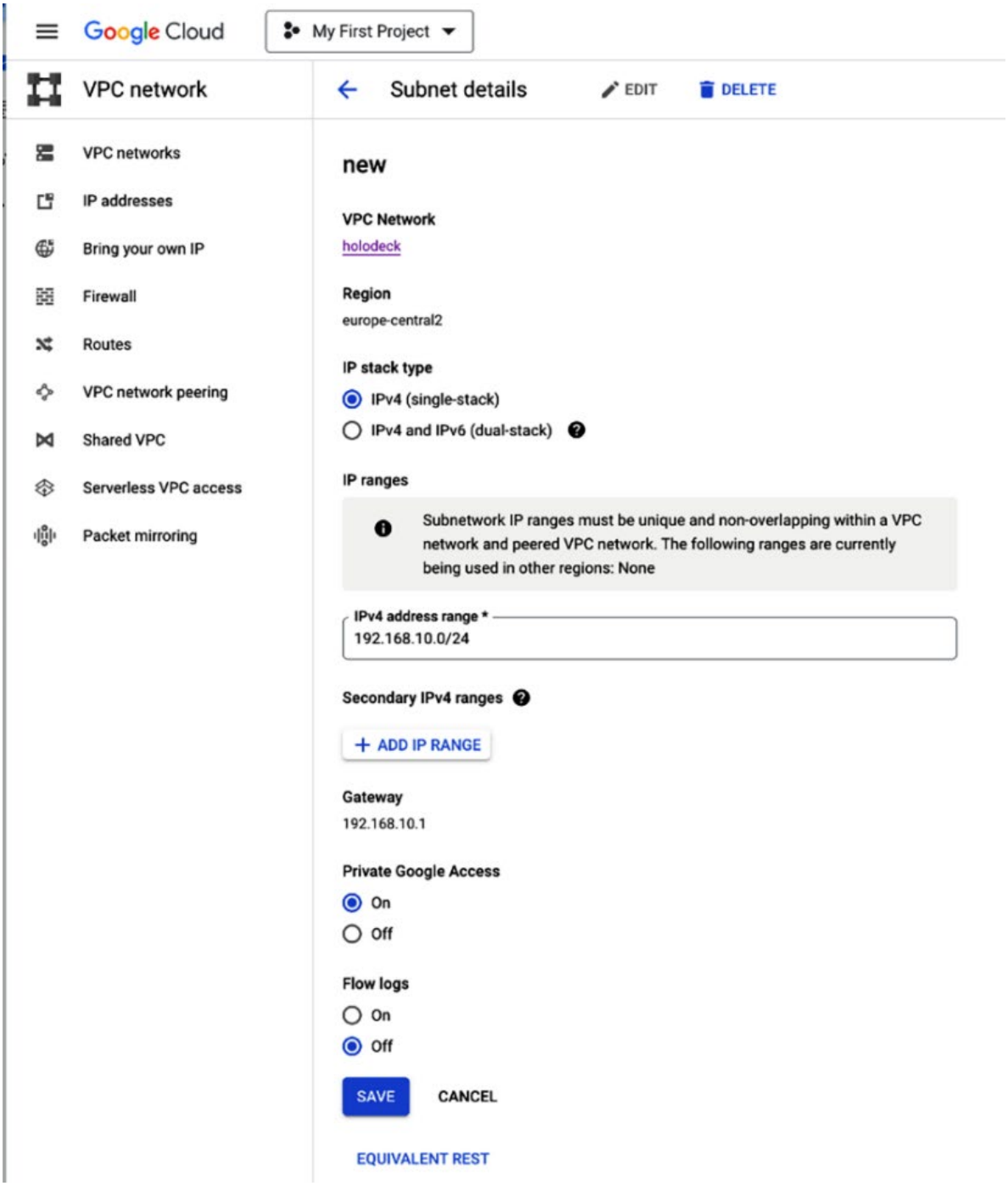


Figure 8.6 – Configuring subnet for Private Google Access

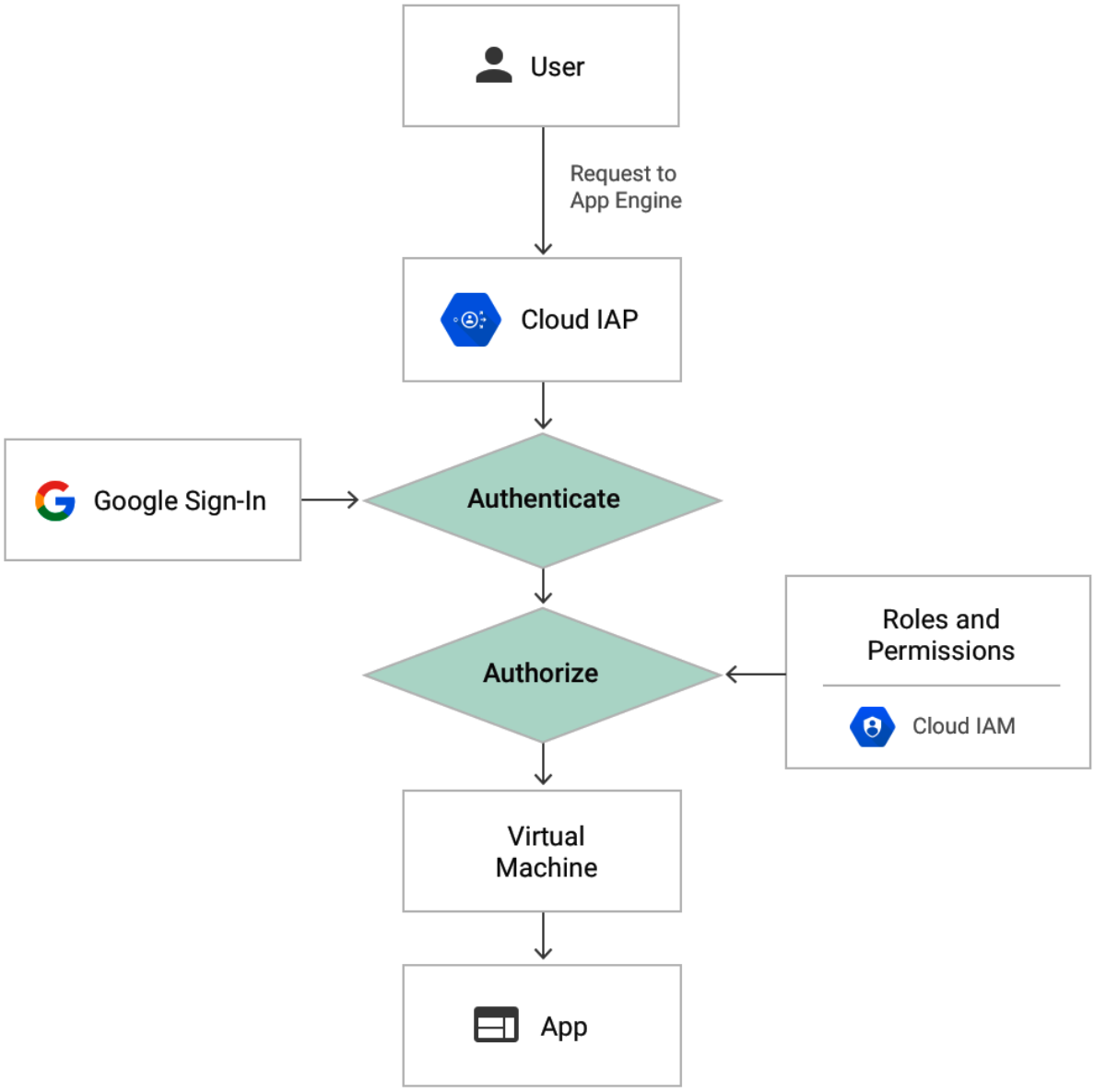


Figure 8.7 – How IAP works with App Engine

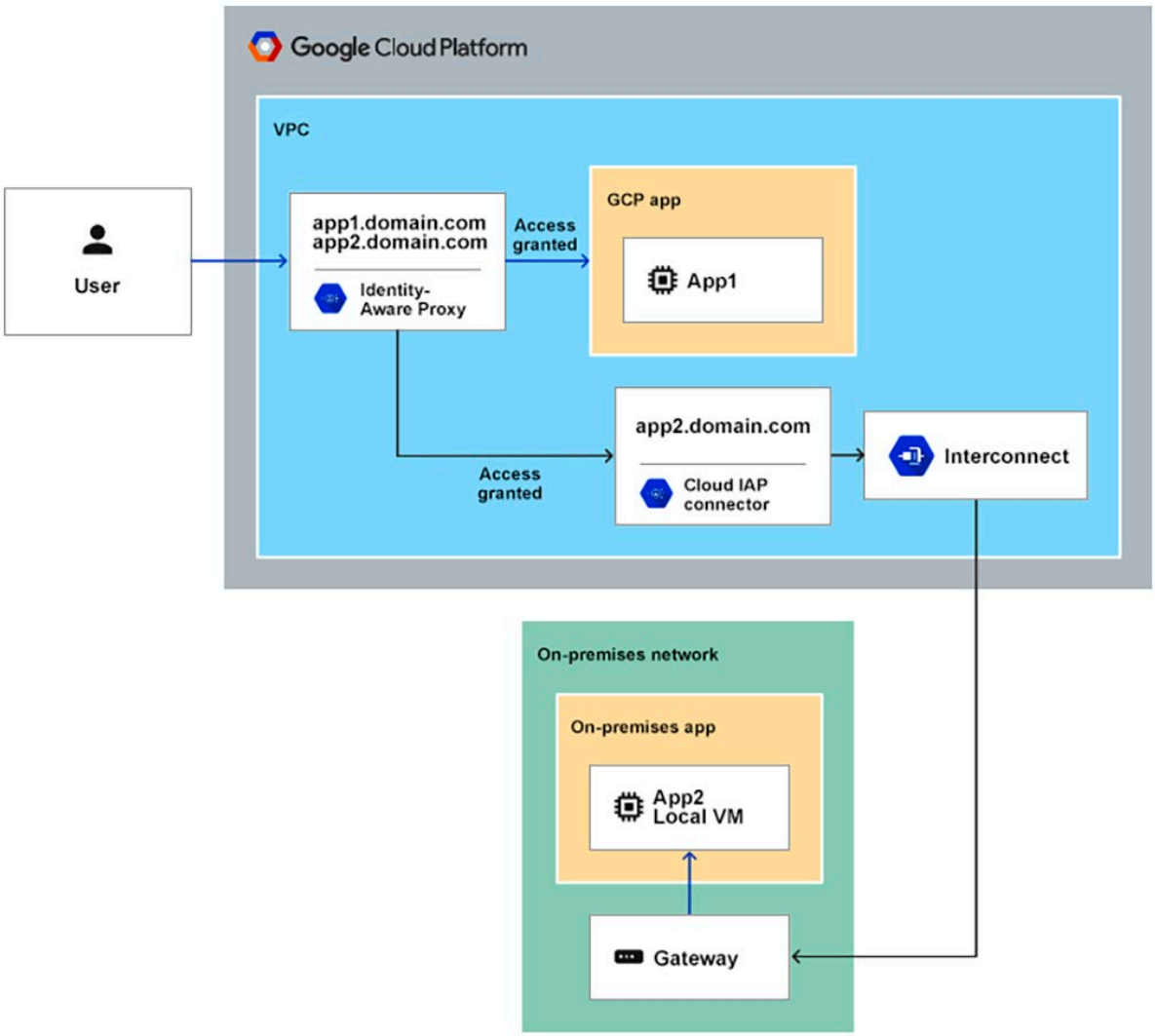


Figure 8.8 – How IAP for on-premises works

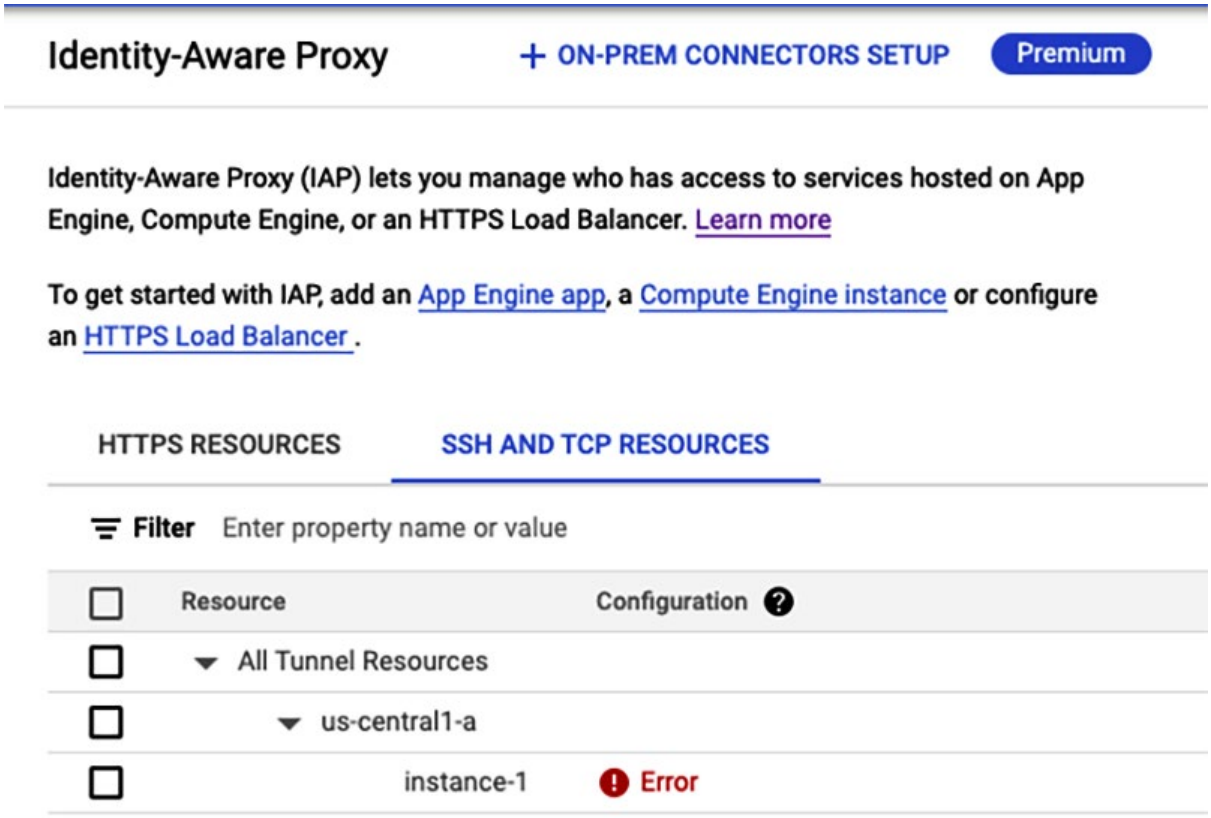


Figure 8.9 – The Identity-Aware Proxy dashboard

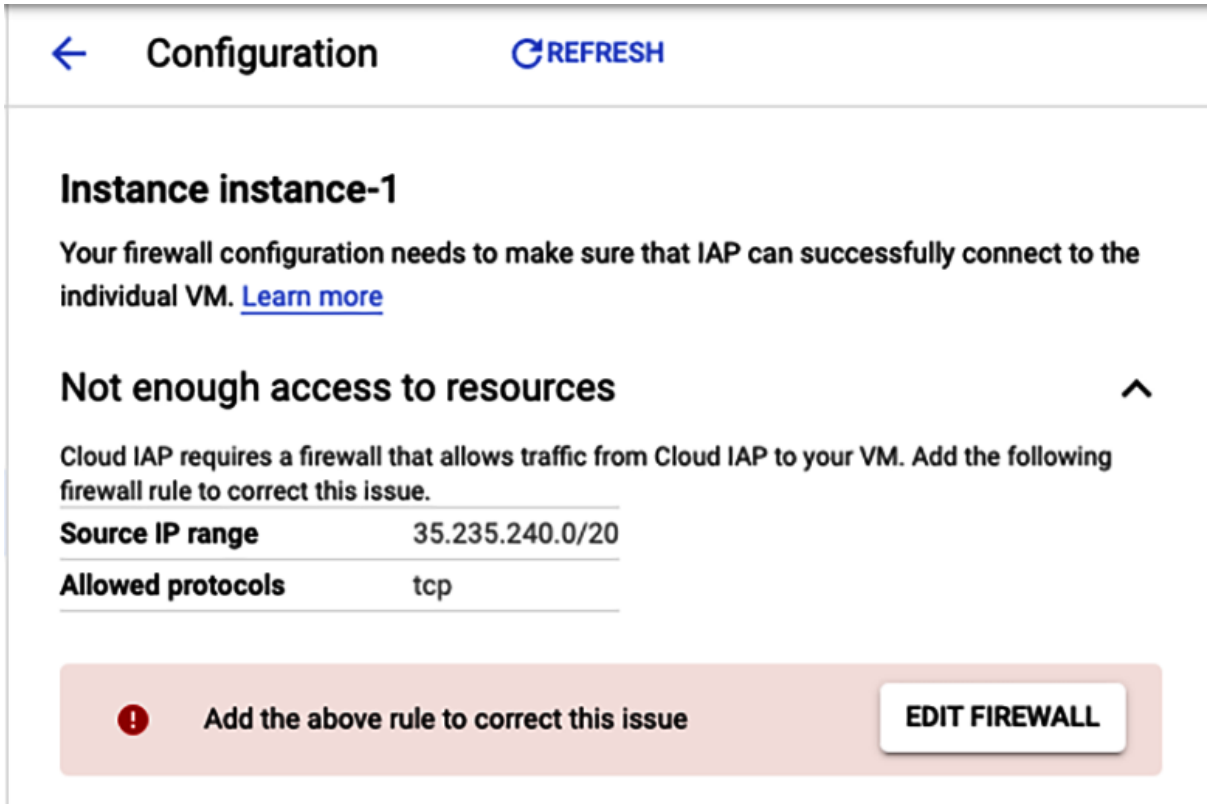


Figure 8.10 – Correcting a firewall configuration for IAP

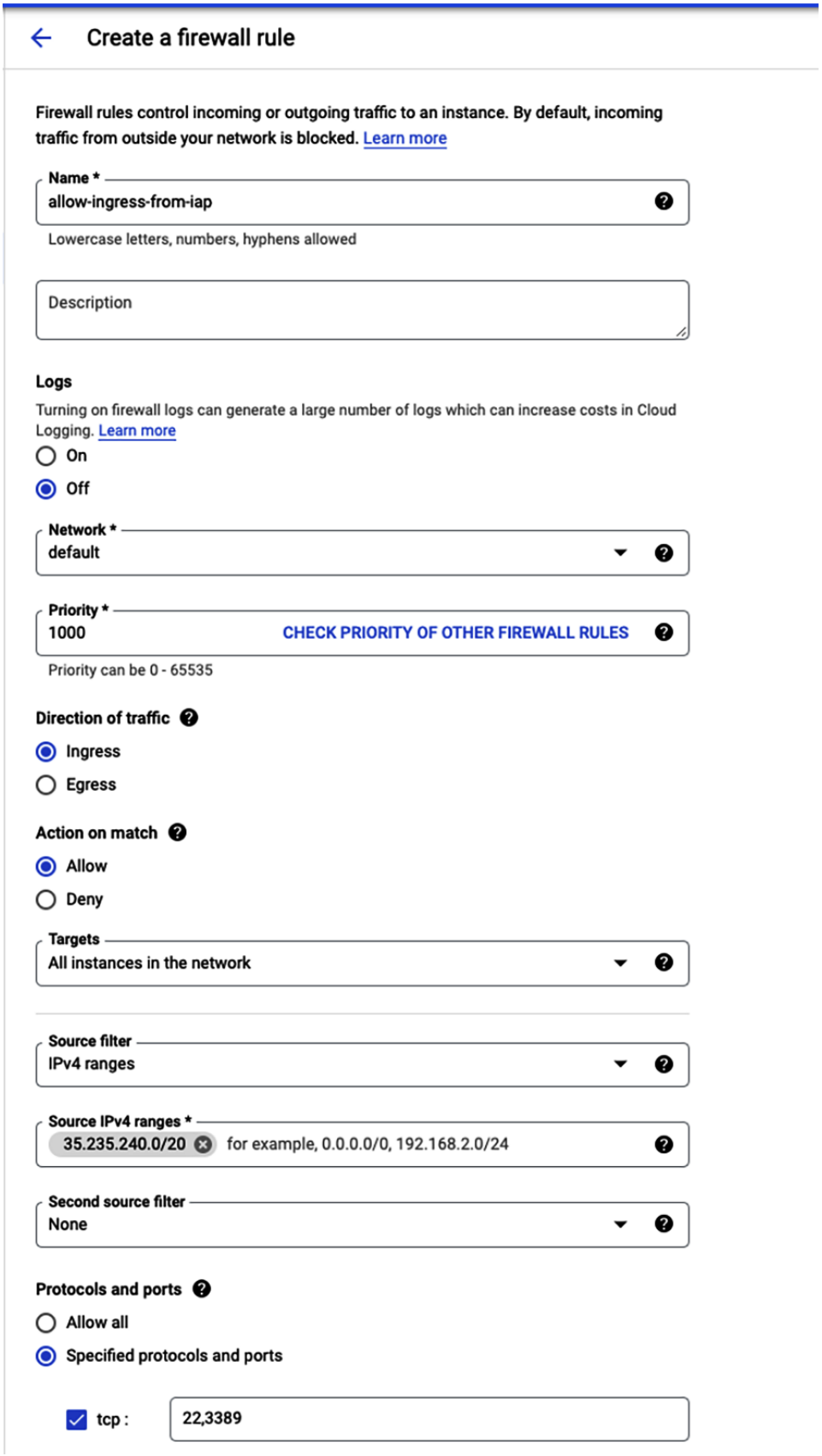


Figure 8.11 – Creating a firewall rule to enable IAP access

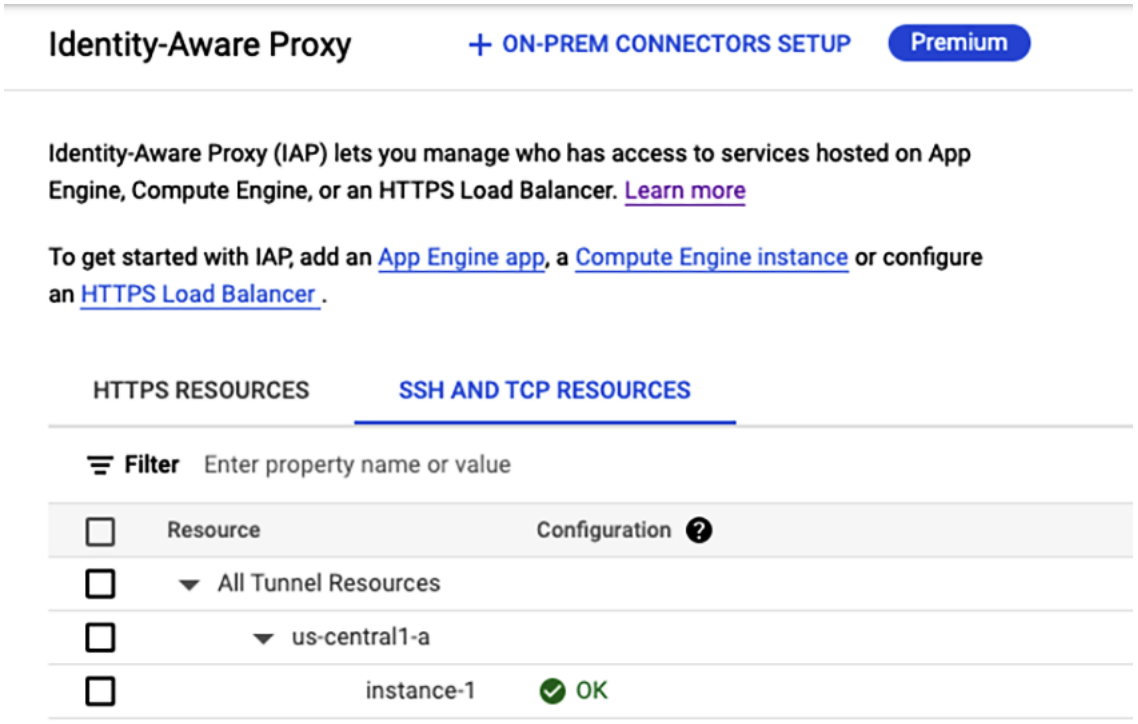


Figure 8.12 – SSH and TCP resources after creating the firewall rule successfully

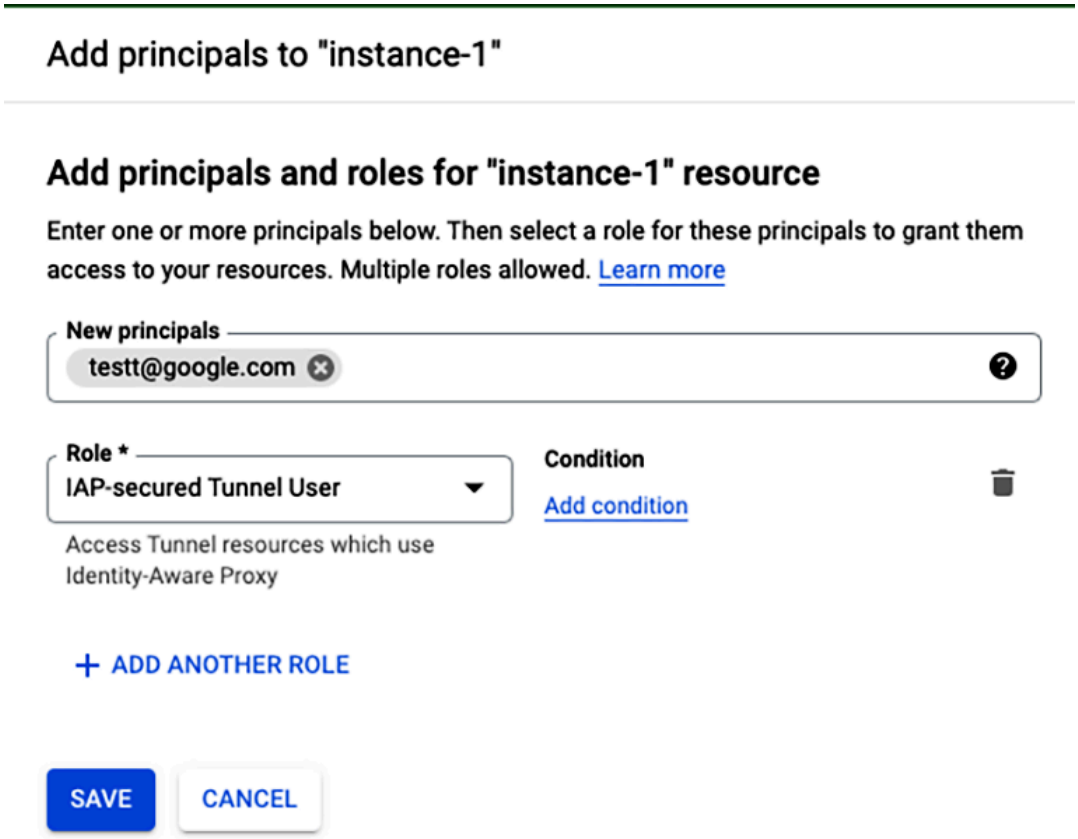


Figure 8.13 – Adding a principal and applying the IAP-secured Tunnel User role

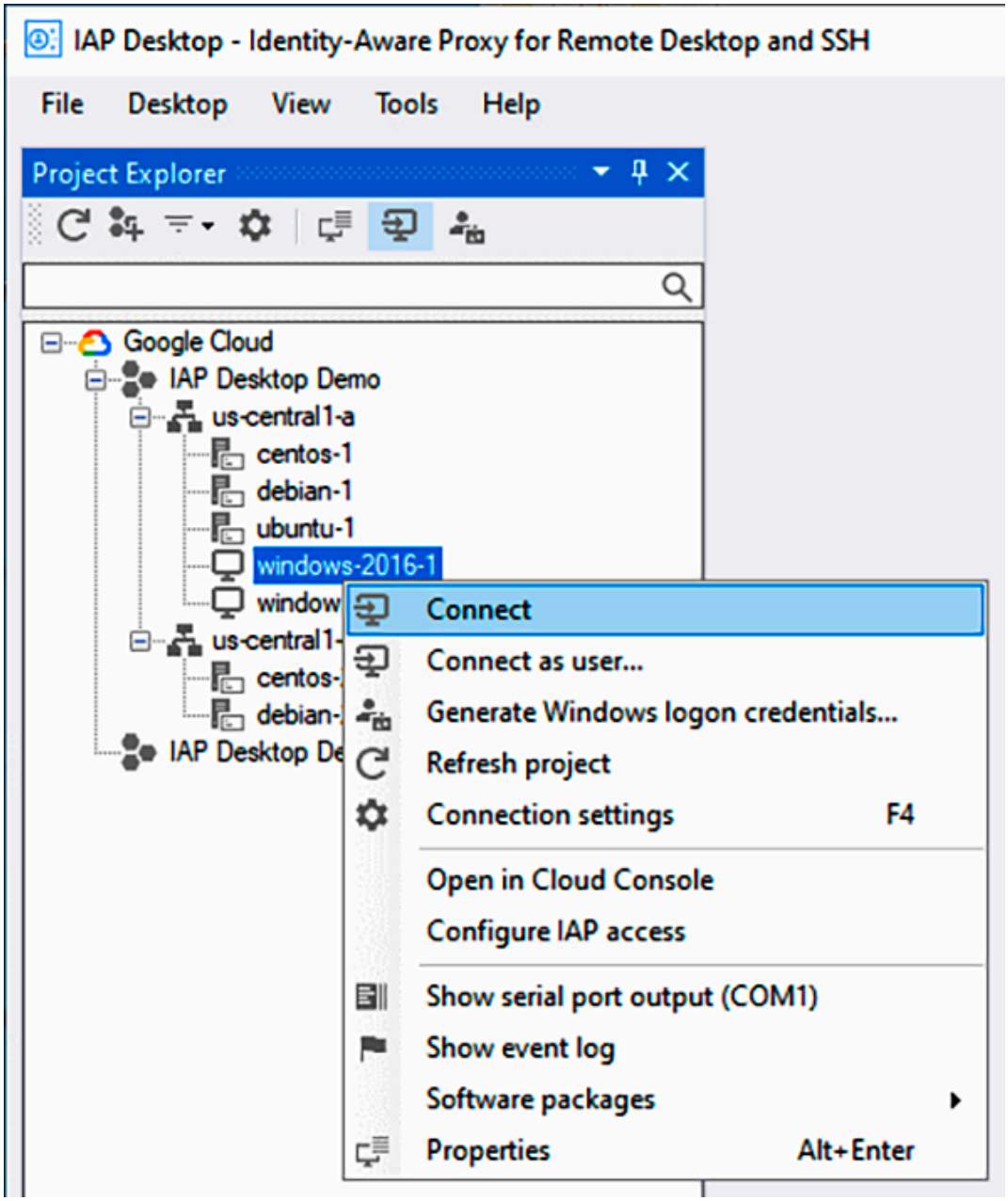


Figure 8.14 – Configuring IAP Desktop for IAP

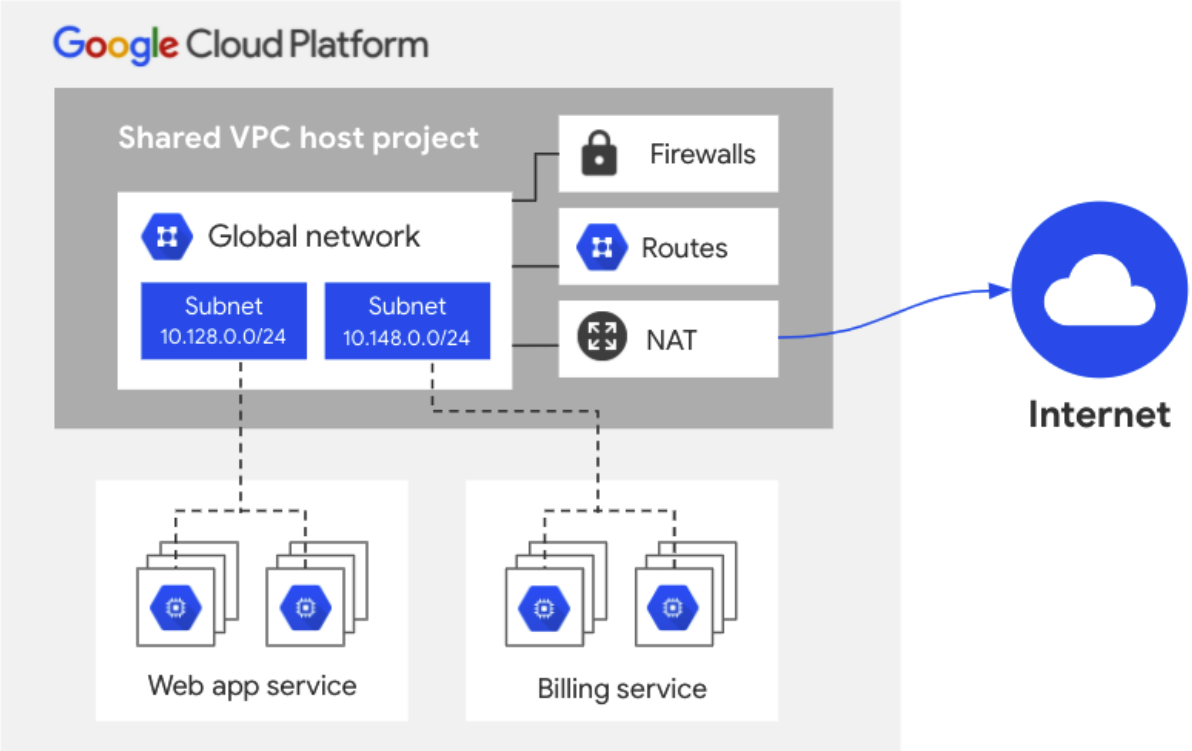


Figure 8.15 – Cloud NAT allowing outbound connections only to the internet

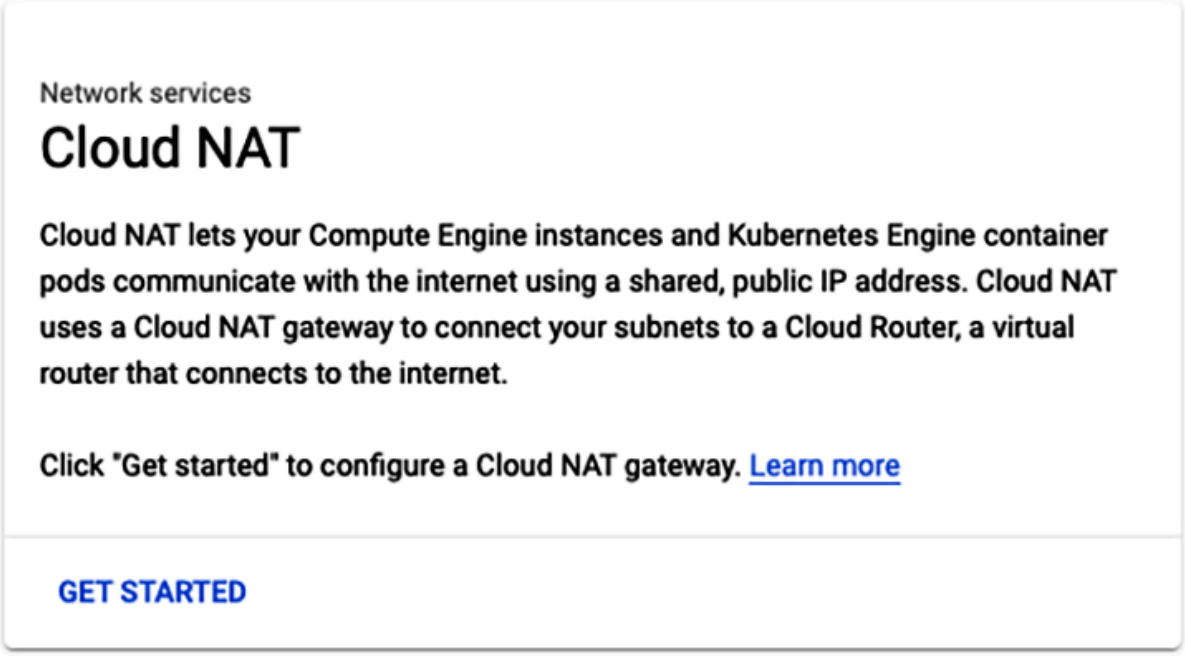


Figure 8.16 – Getting started with Cloud NAT

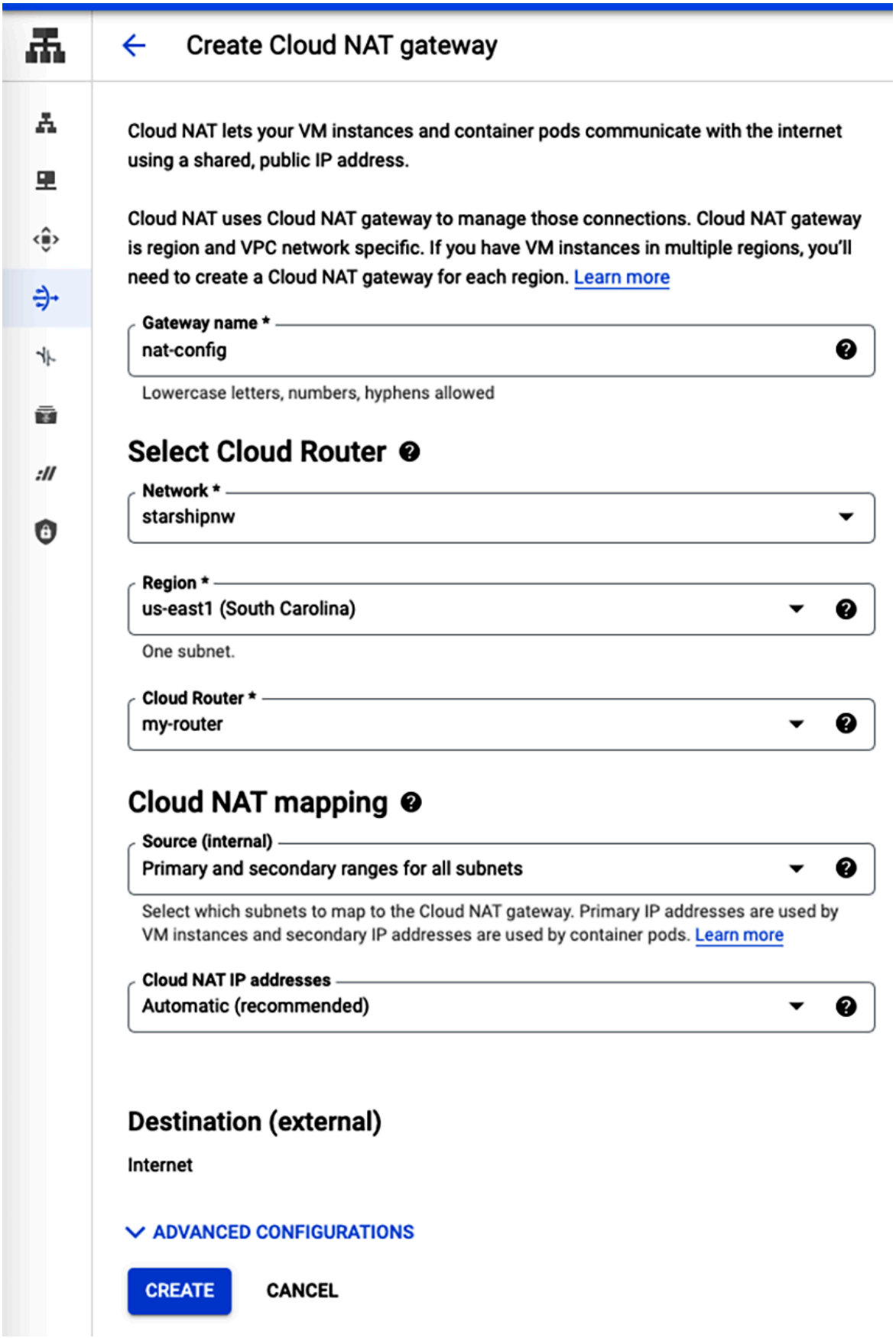


Figure 8.17 – Configuration to create a Cloud NAT gateway

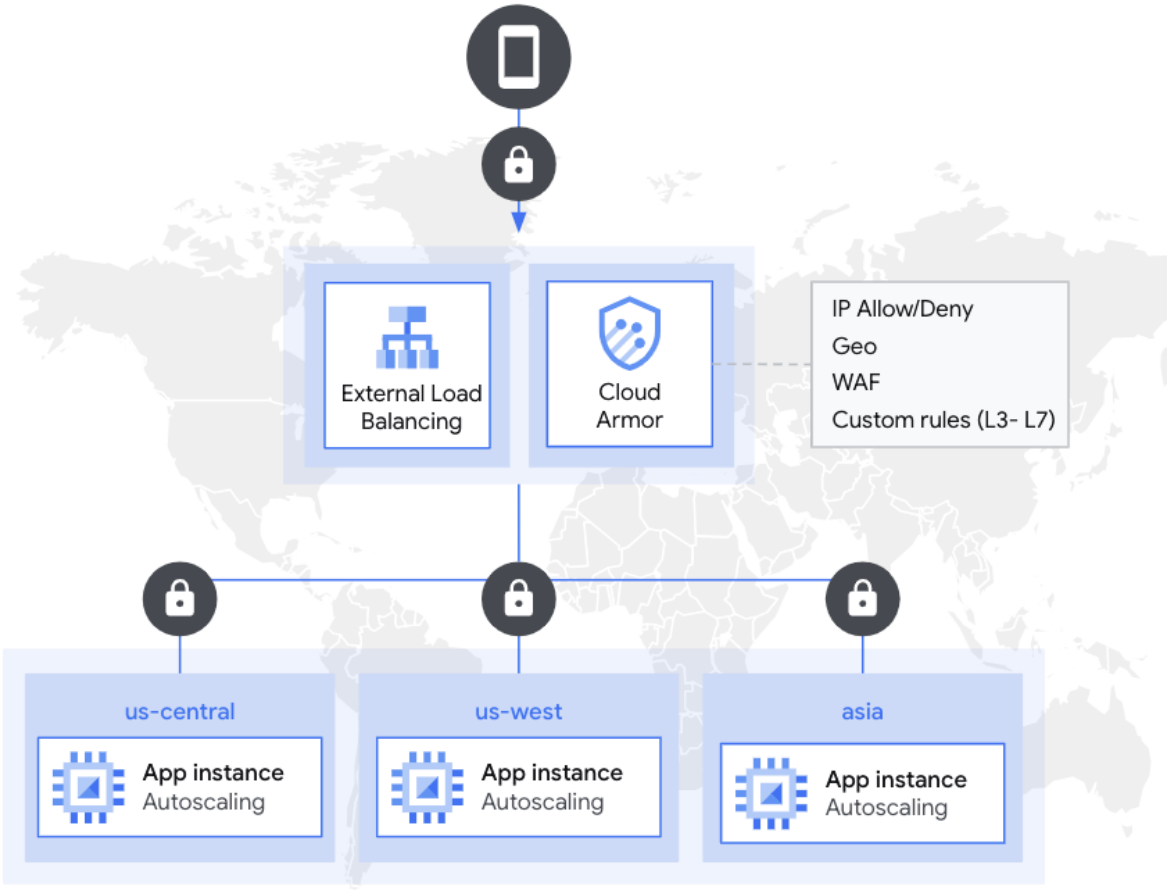


Figure 8.18 – How Google Cloud Armor secures your infrastructure

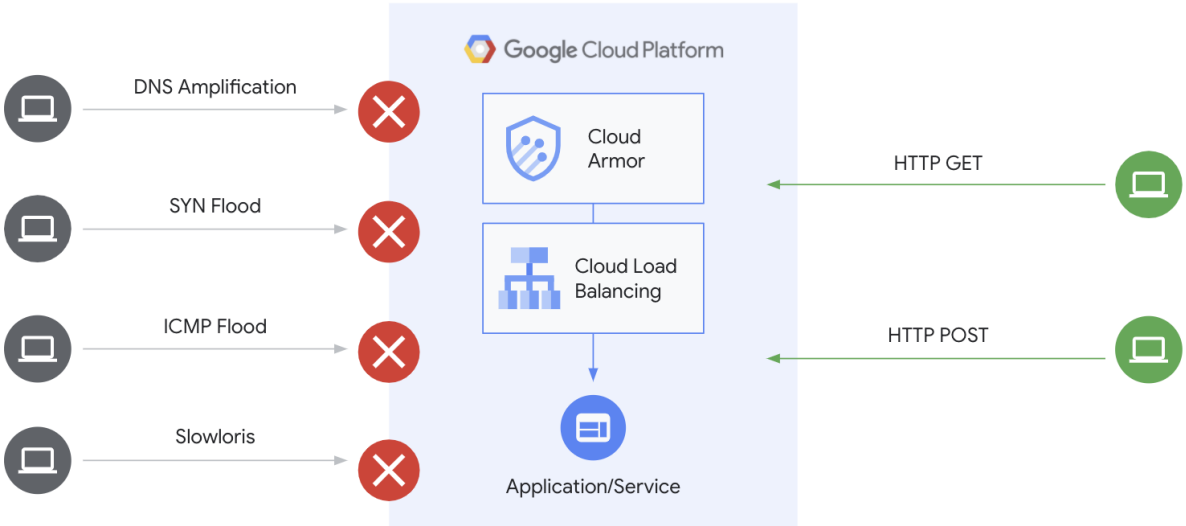


Figure 8.19 – DDoS protection against volumetric attacks

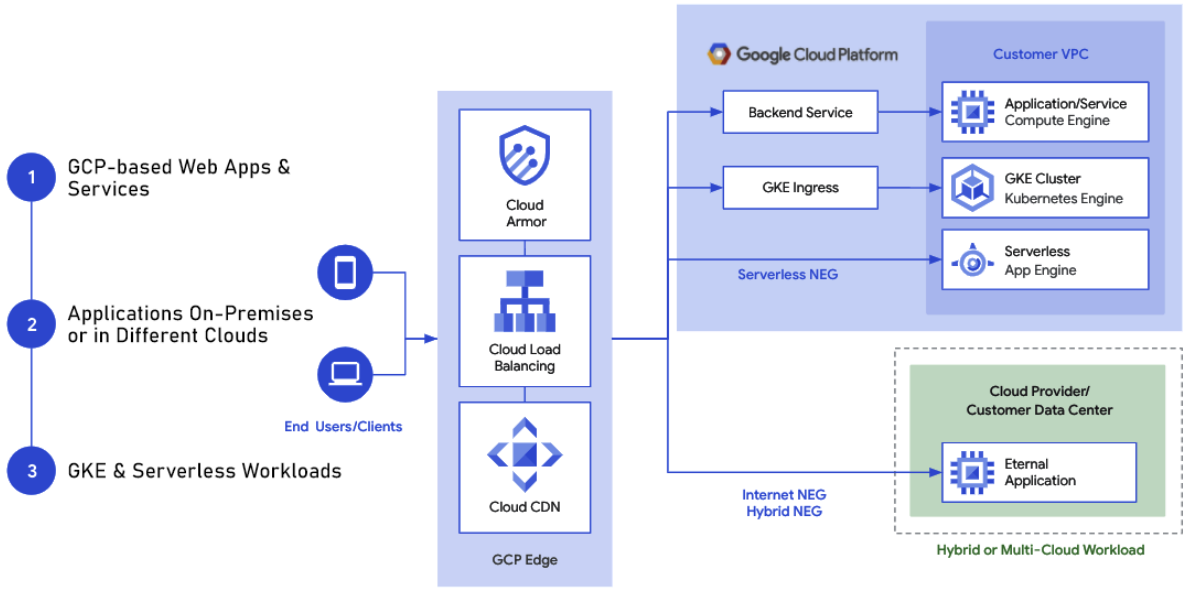


Figure 8.20 – Cloud Armor deployment models

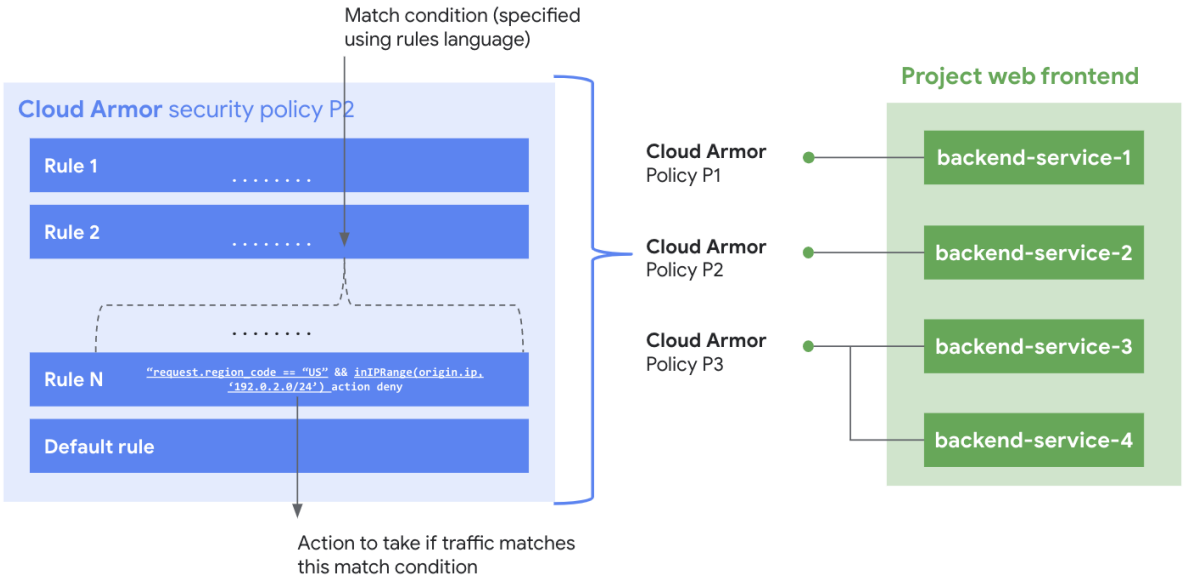


Figure 8.21 – Cloud Armor security policies

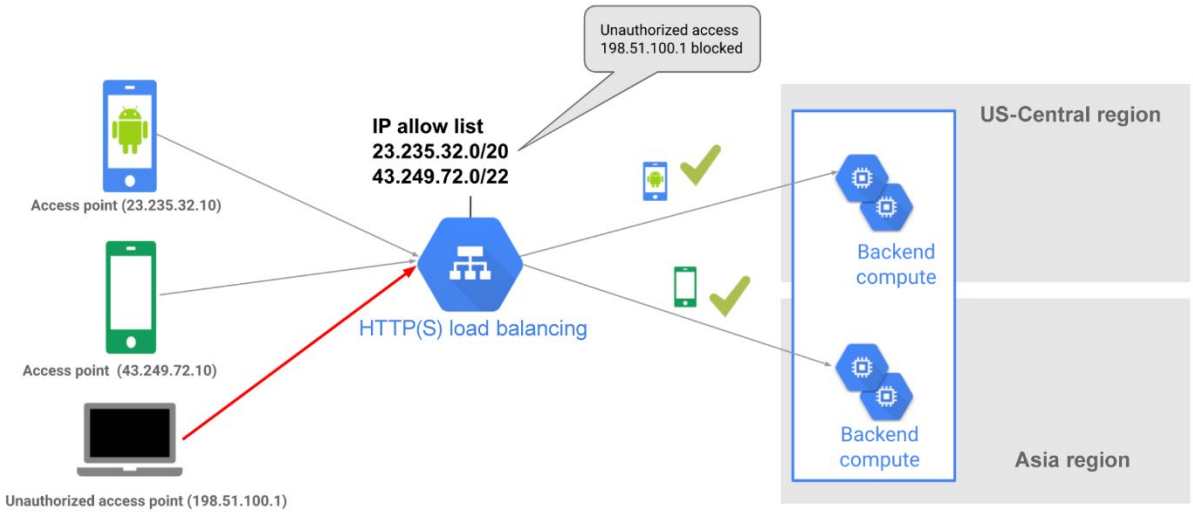


Figure 8.22 – Cloud Armor named IP list

Chapter 9: Google Cloud Key Management Service

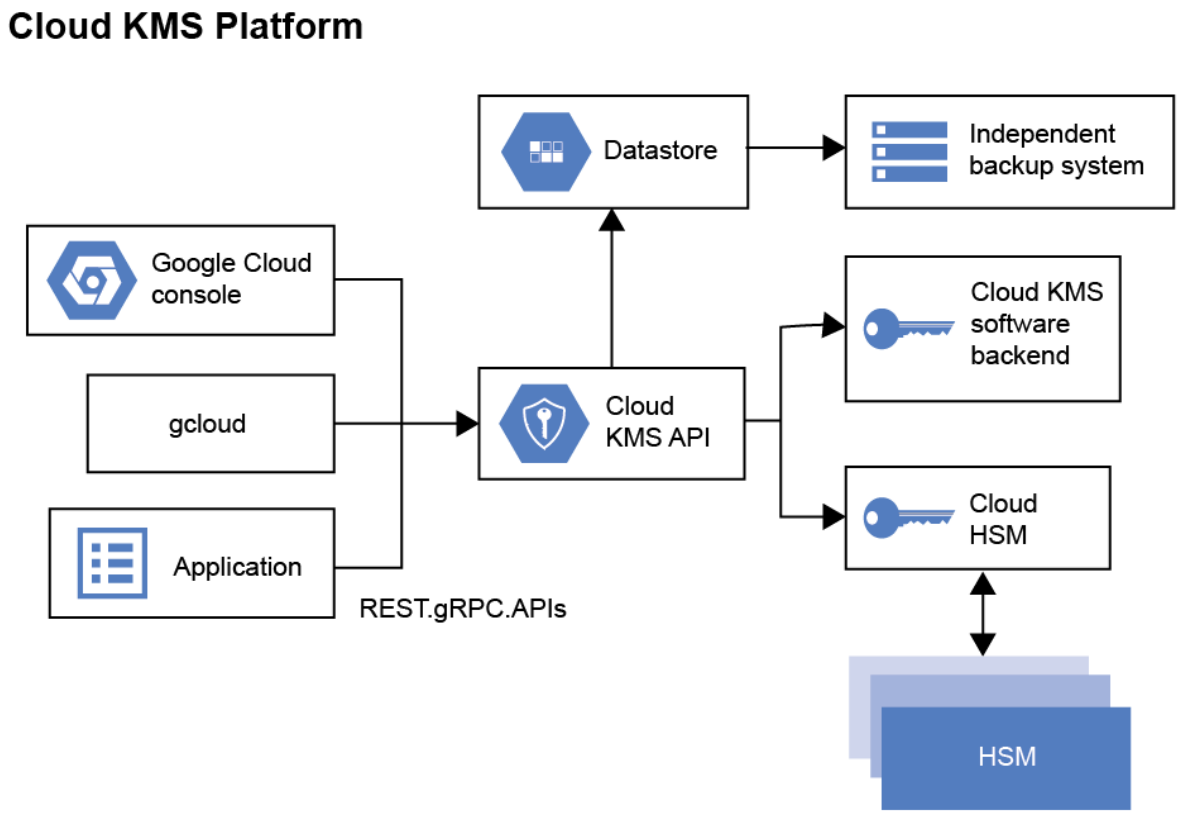


Figure 9.1 – The Cloud KMS architecture

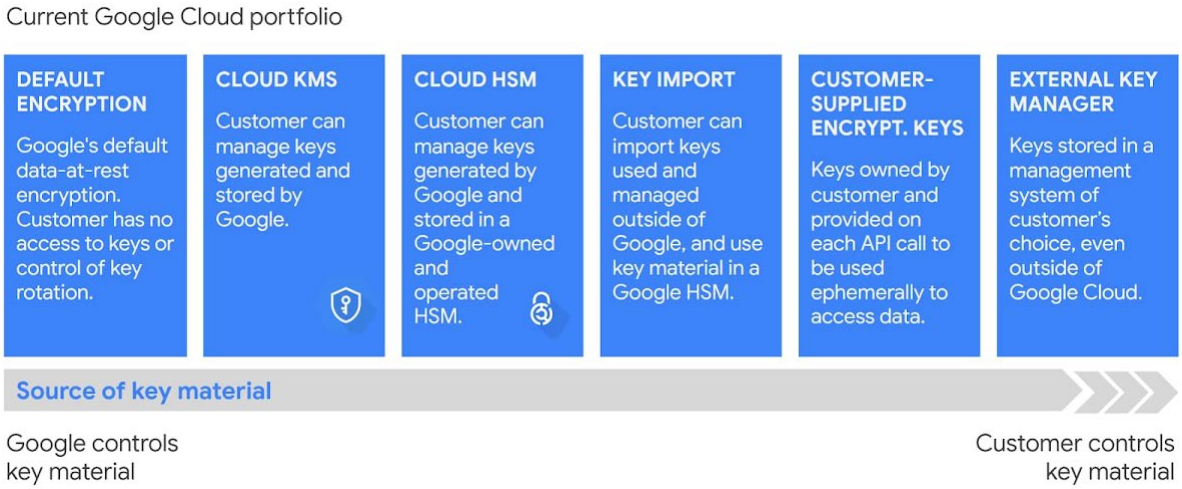


Figure 9.2 – Google Cloud encryption offerings

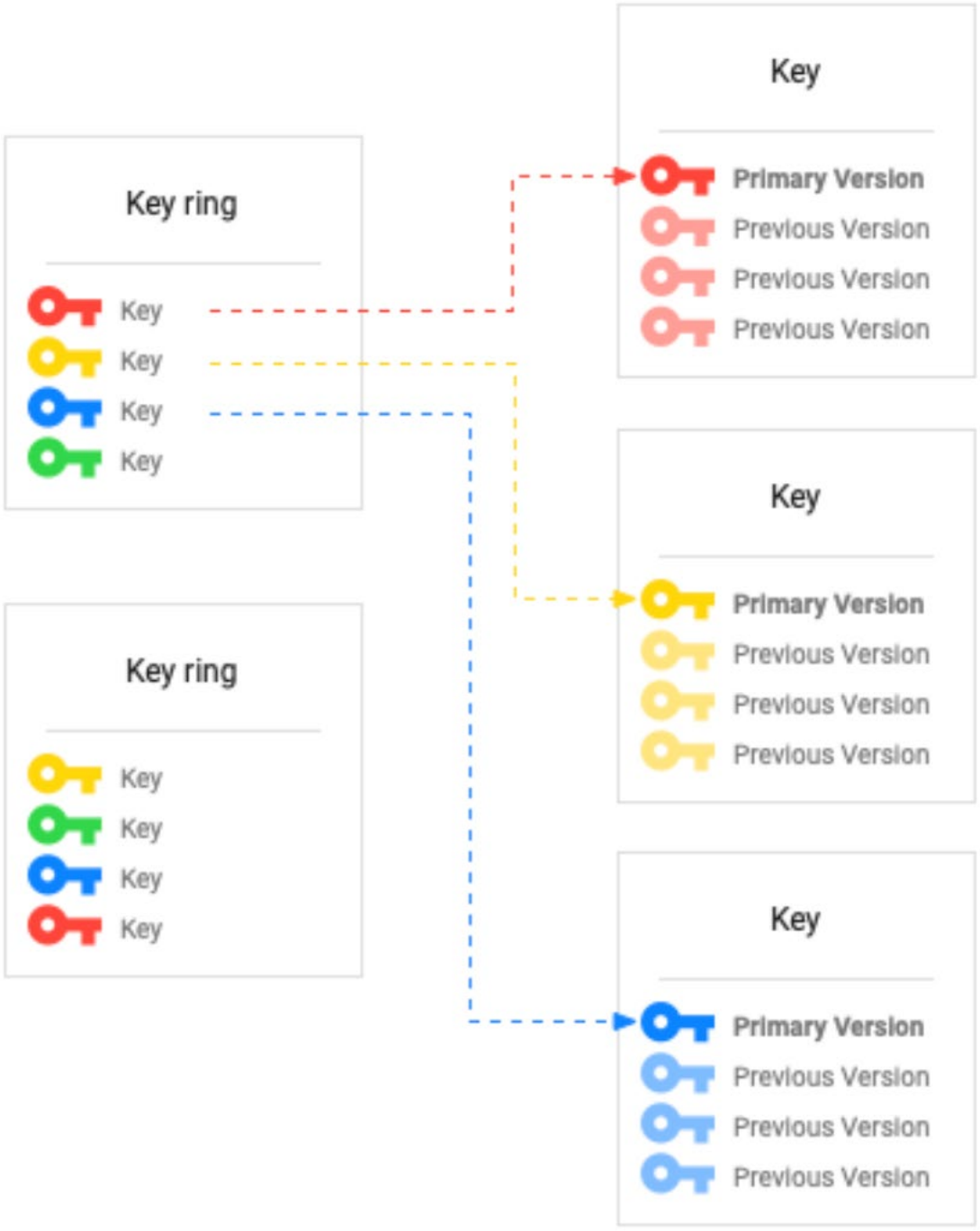


Figure 9.3 – Key structure

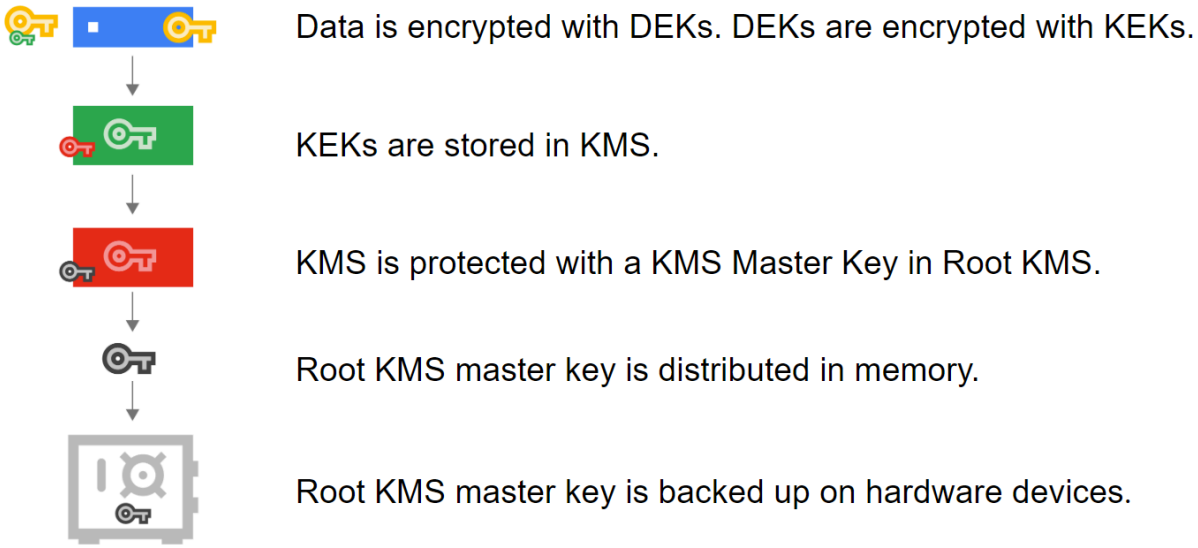


Figure 9.4 – Key hierarchy

Figure 9.5 – Envelope encryption

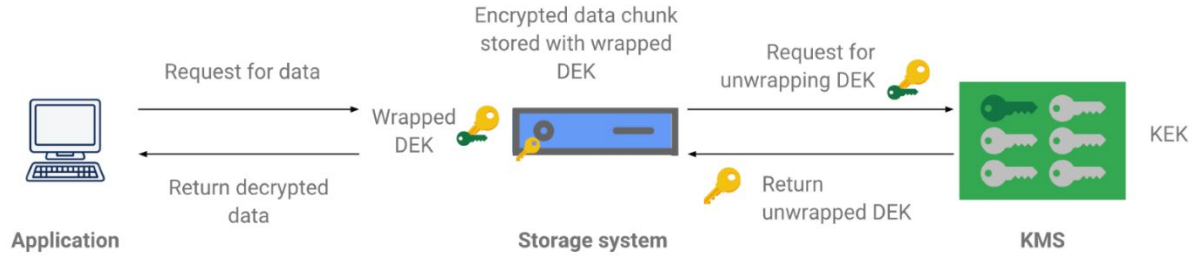


Figure 9.6 – Envelope decryption

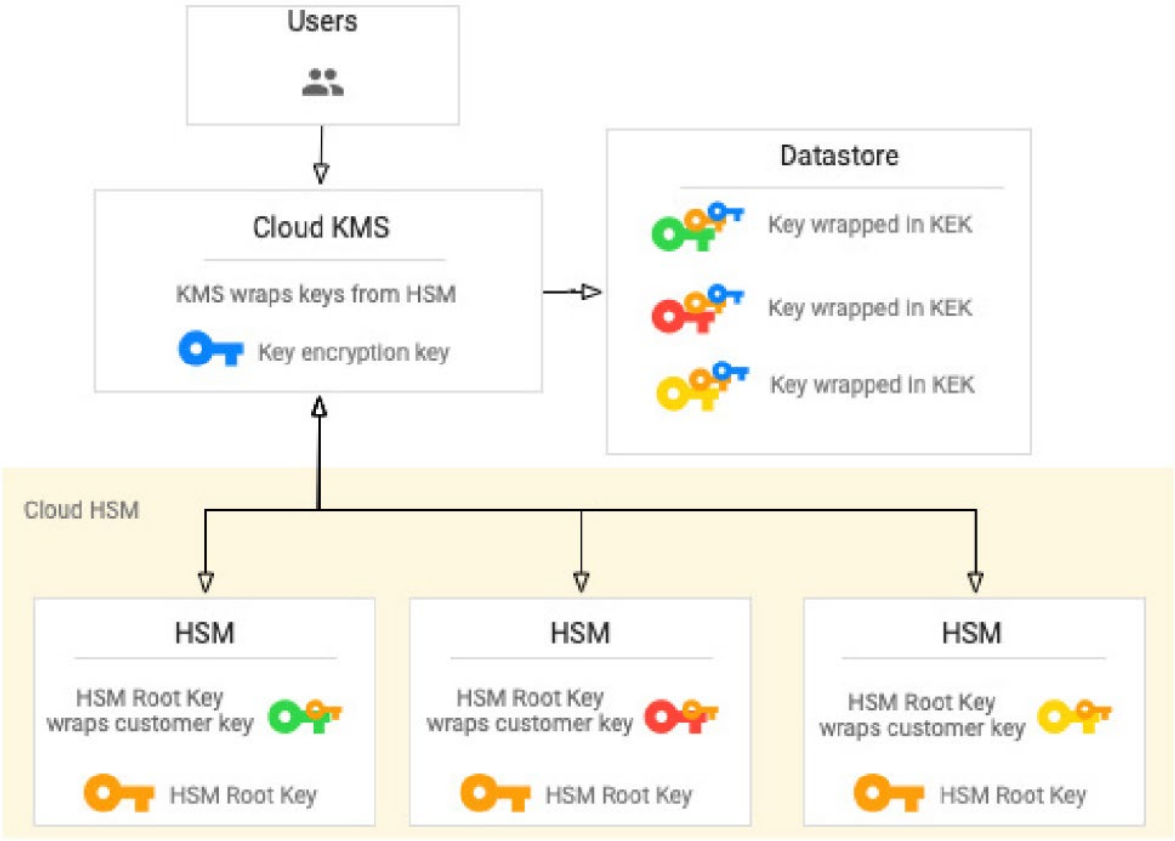


Figure 9.7 – HSM key hierarchy

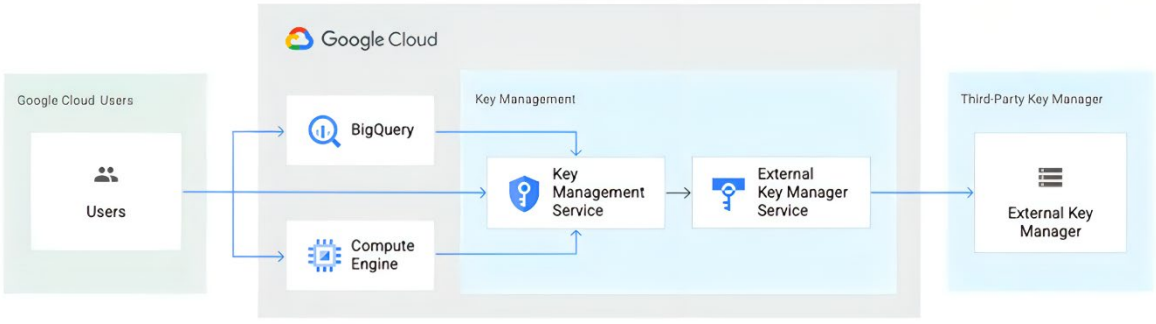


Figure 9.8 – Cloud EKM architecture

Chapter 10: Cloud Data Loss Prevention

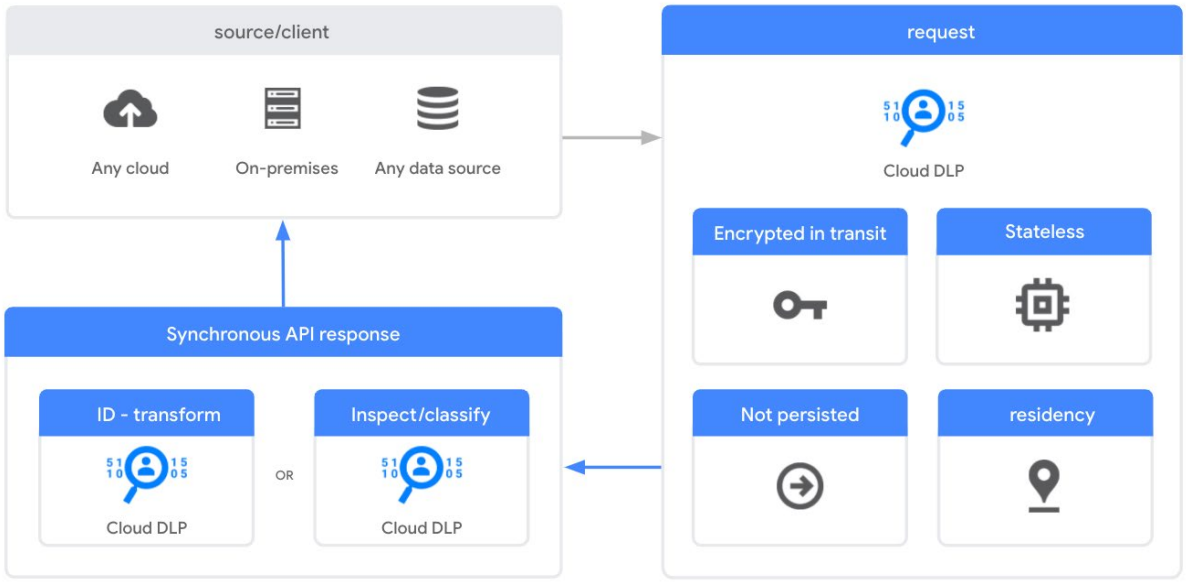


Figure 10.1 – Content method architecture

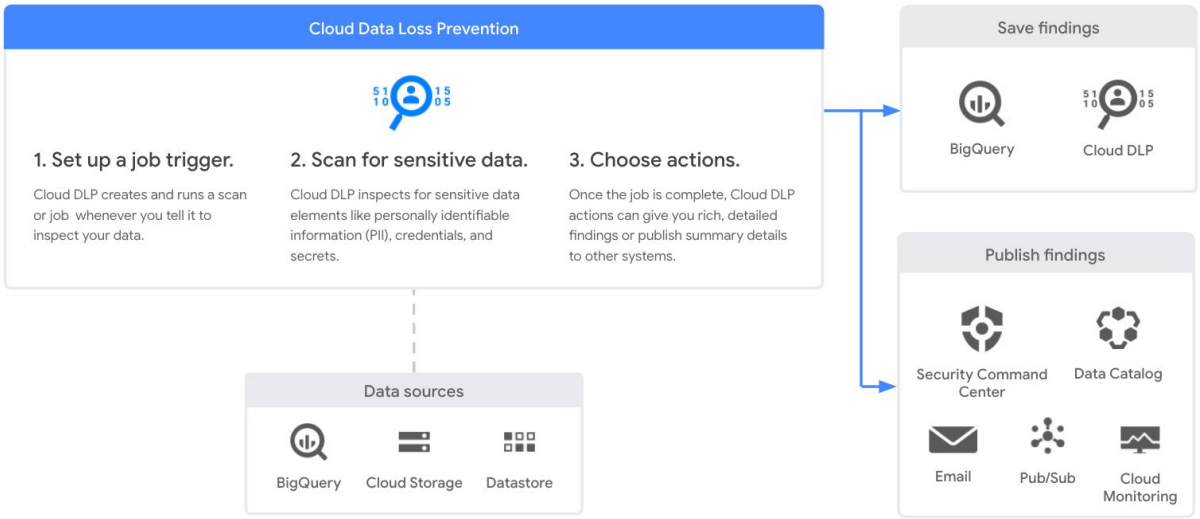


Figure 10.2 – Storage method architecture

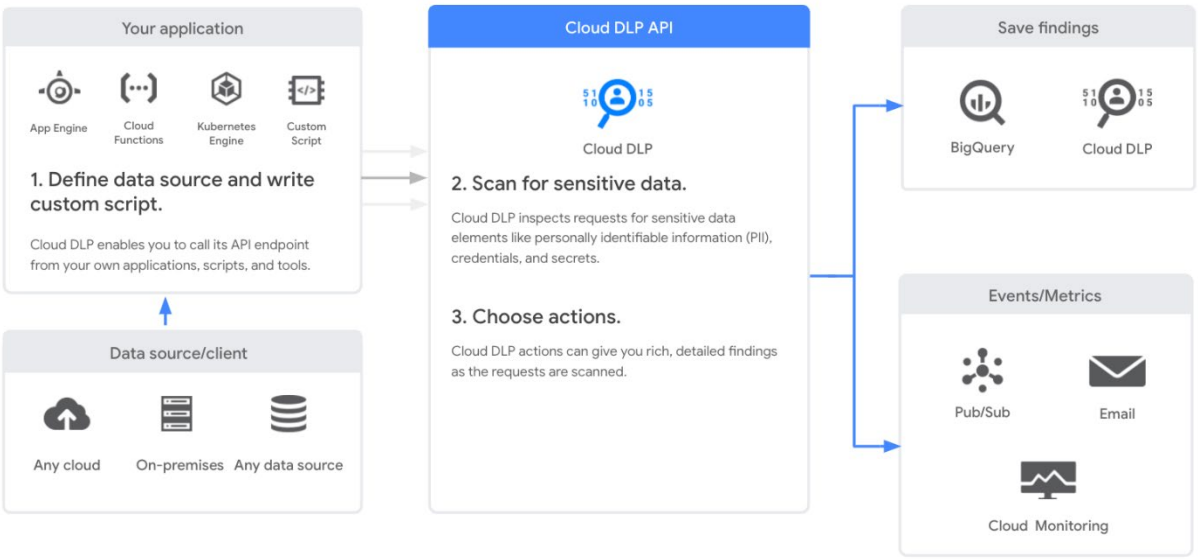


Figure 10.3 – Hybrid inspection architecture

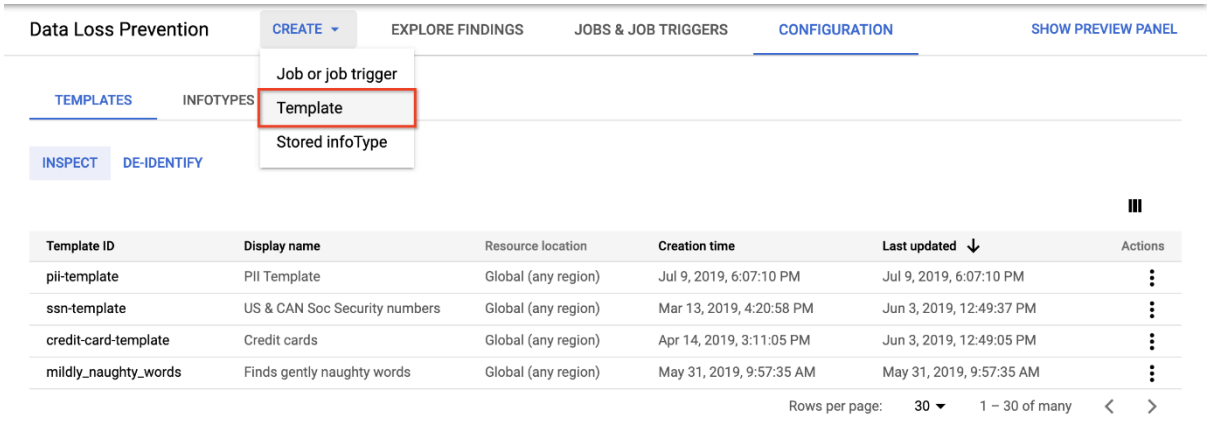


Figure 10.4 – Creating a DLP inspection template

Inspection rulesets

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

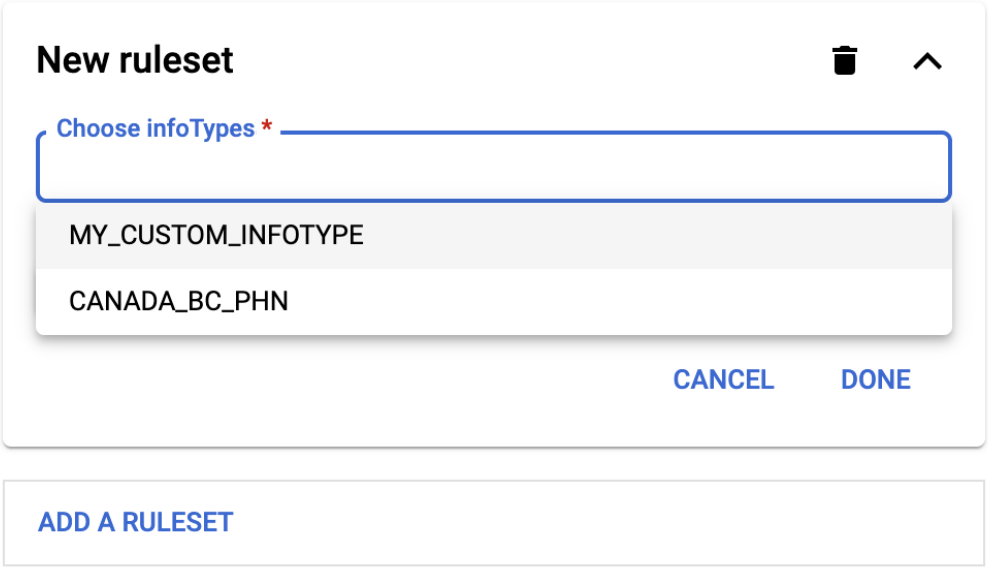


Figure 10.5 – Choosing infoTypes for Inspection rulesets

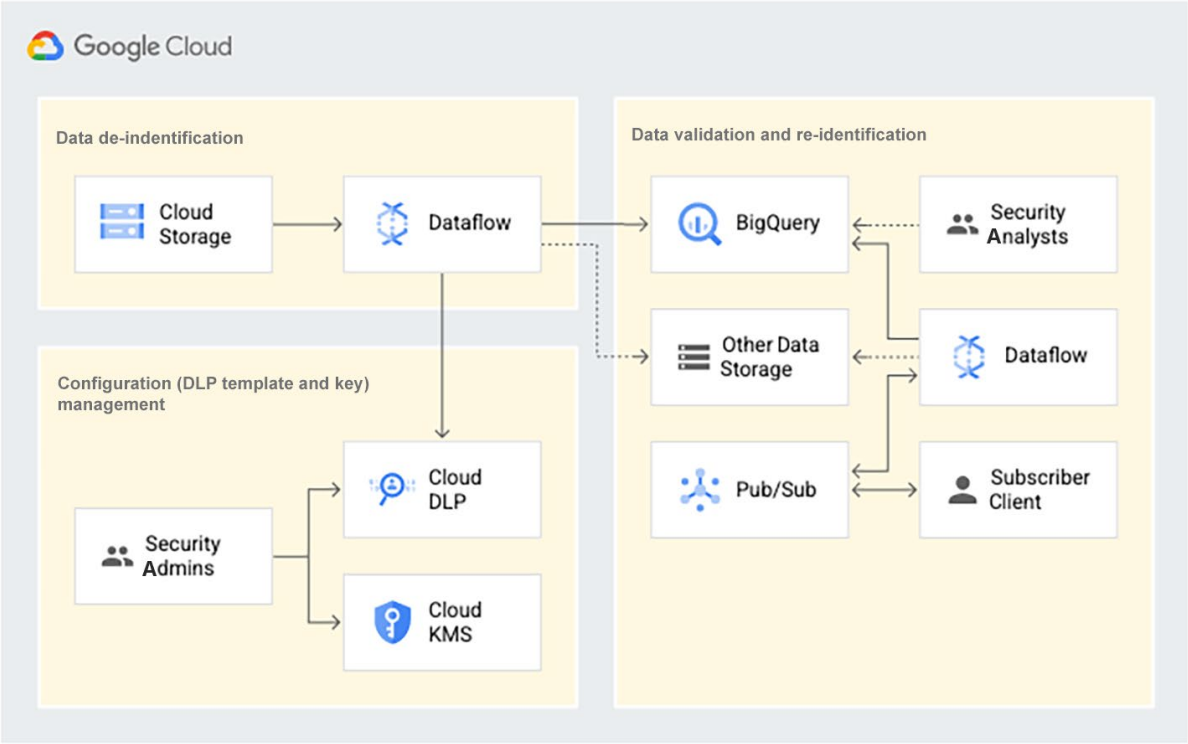


Figure 10.6 – DLP pattern for Dataflow and Data Fusion pipeline

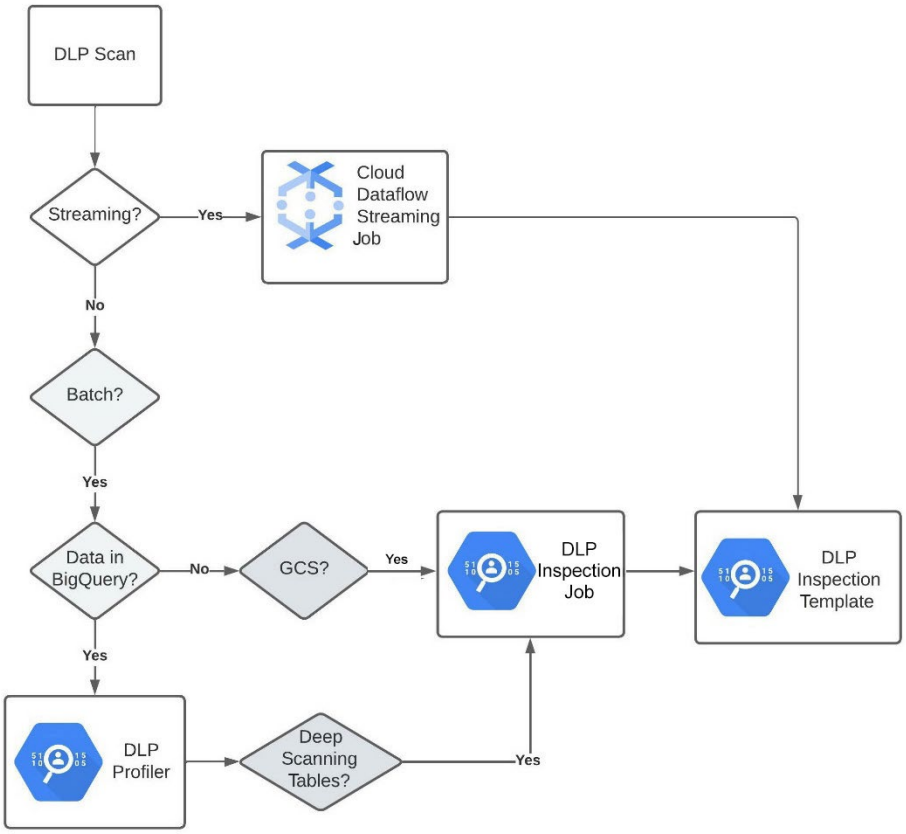


Figure 10.7 – Decision tree for inspection

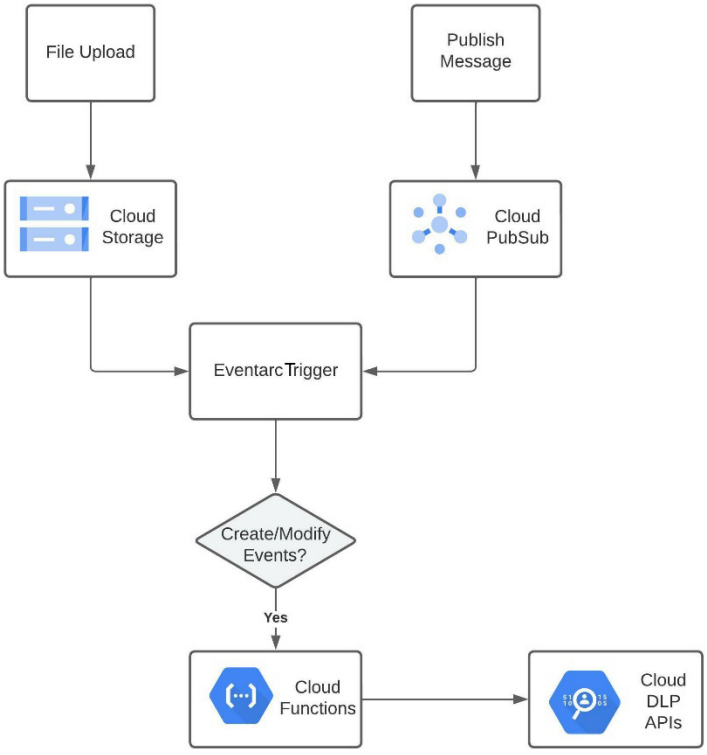


Figure 10.8 – Pattern for new updates

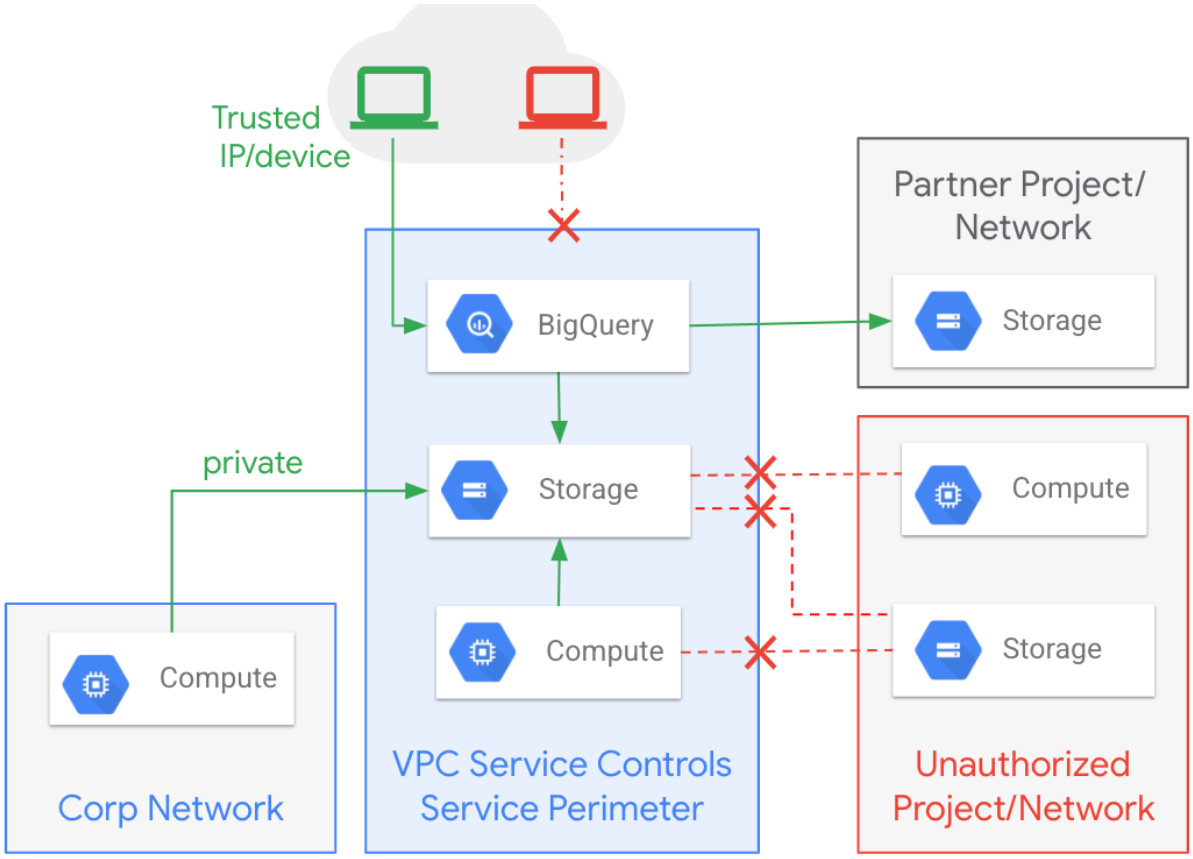


Figure 10.9 – VPC Service Controls architecture

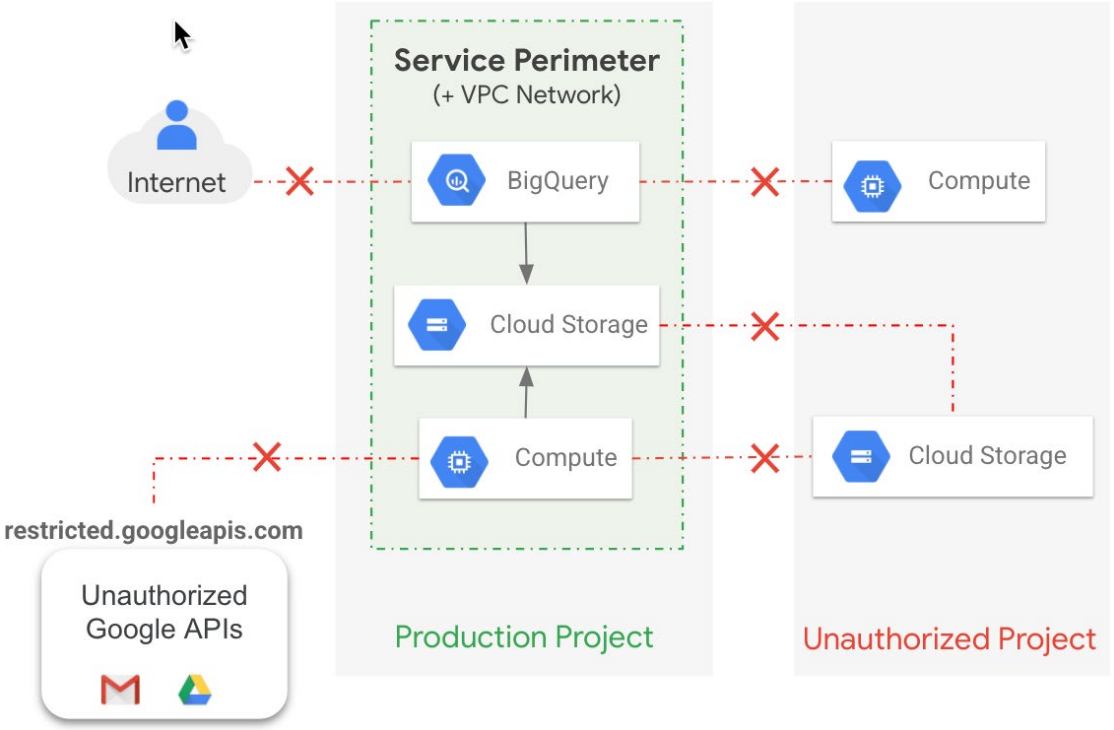


Figure 10.10 – Control APIs

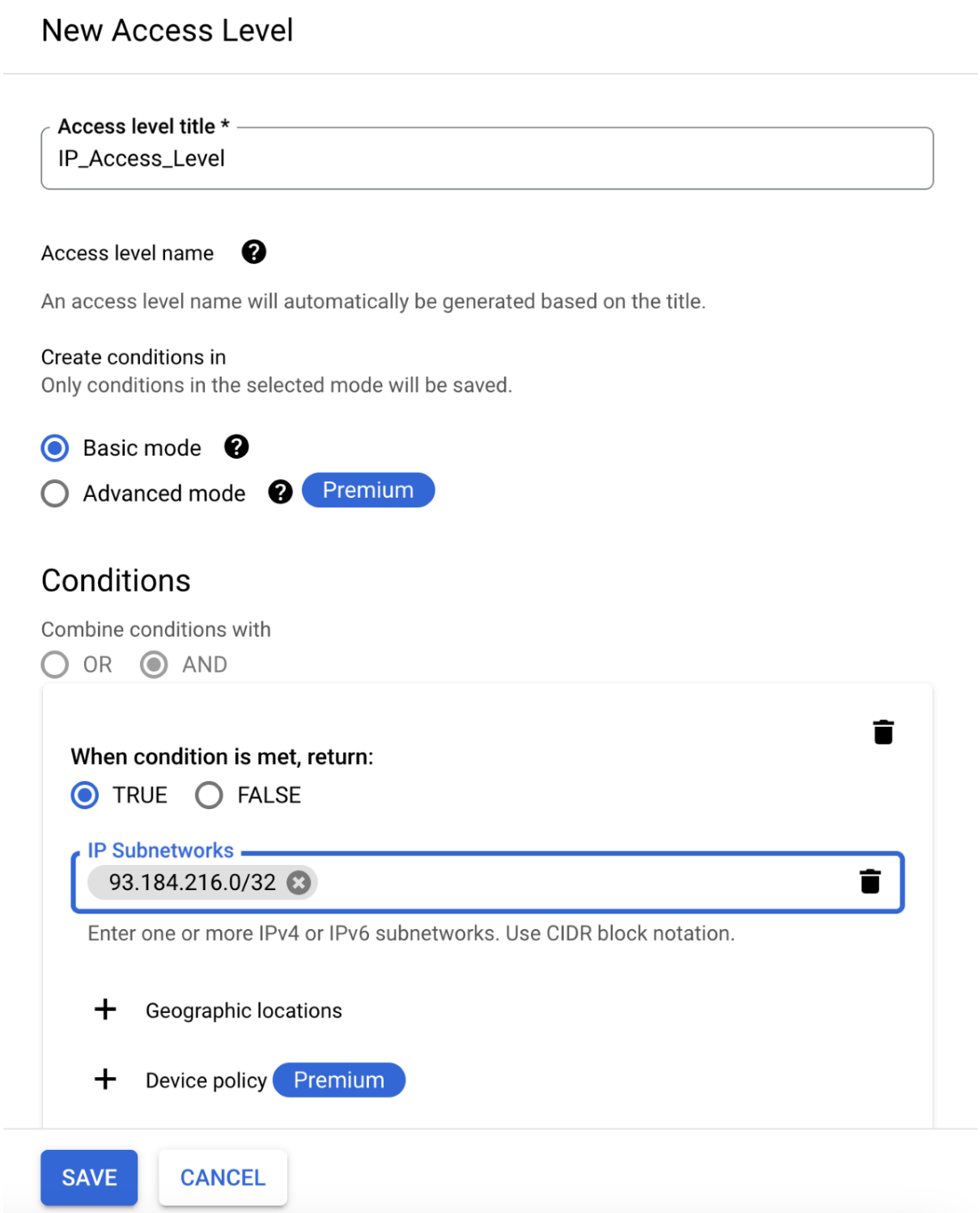


Figure 10.11 – Creating access level

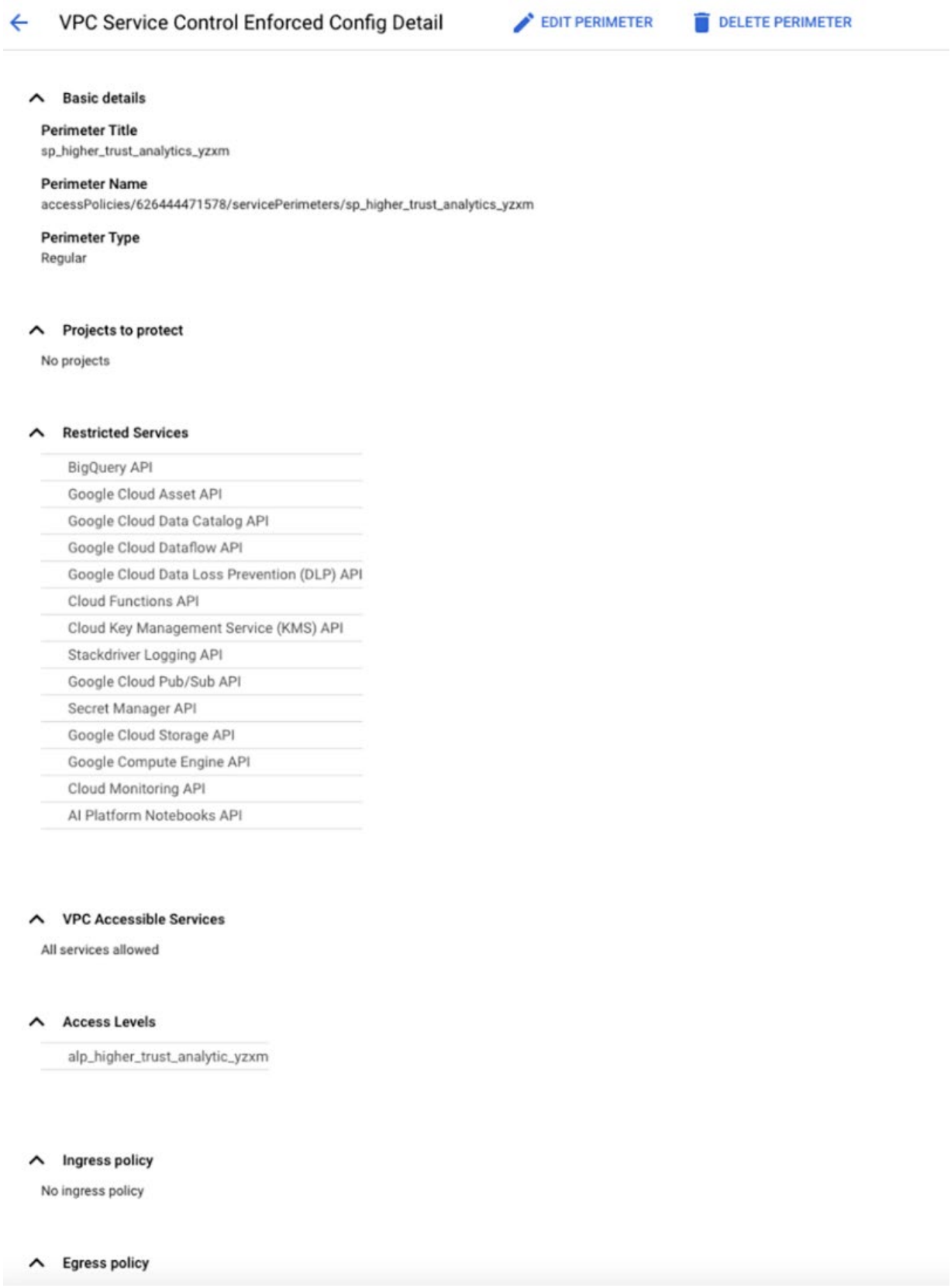


Figure 10.12 – Defining a service perimeter

Chapter 11: Secret Manager

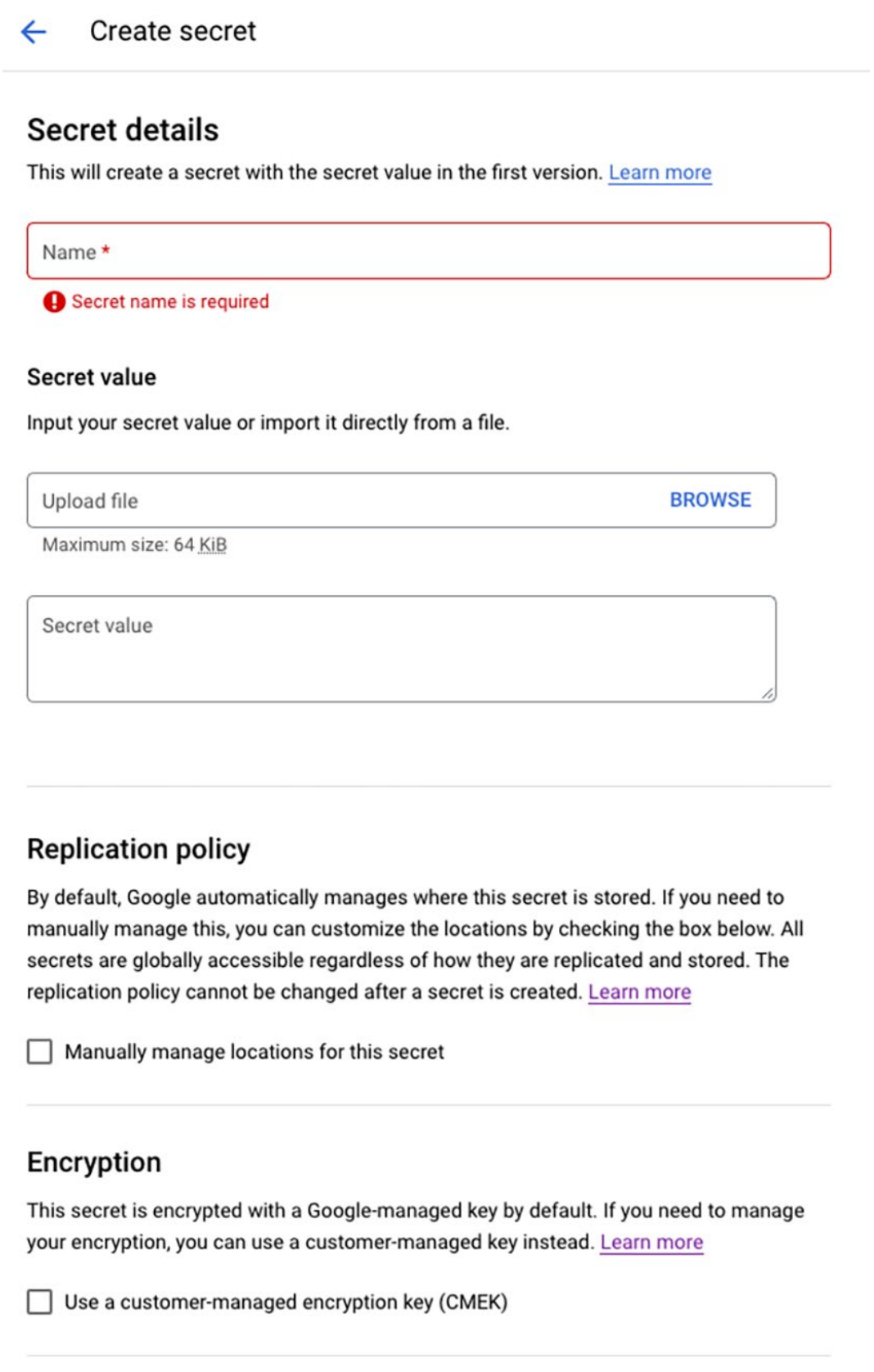


Figure 11.1 – Creating a new secret

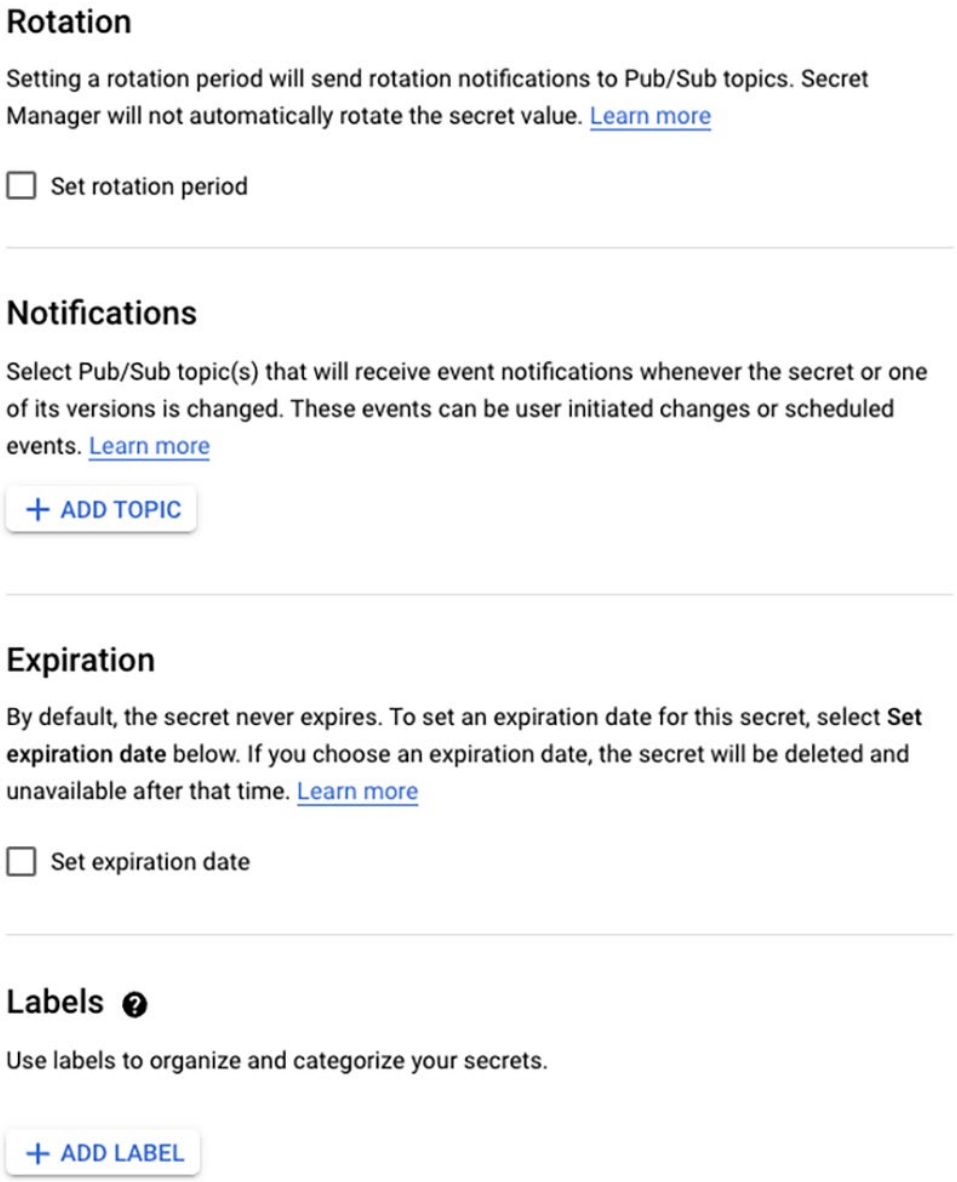


Figure 11.2 – Creating a new secret—rotation period

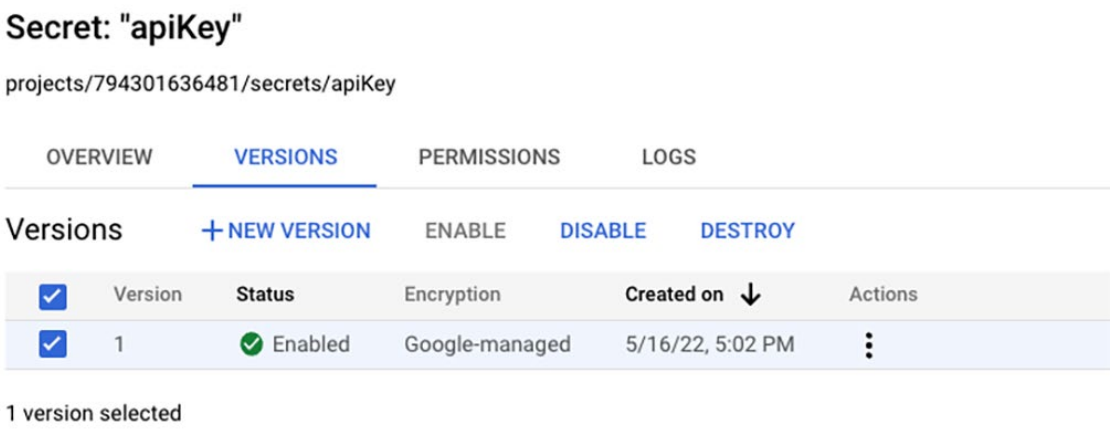


Figure 11.3 – Adding a new secret version

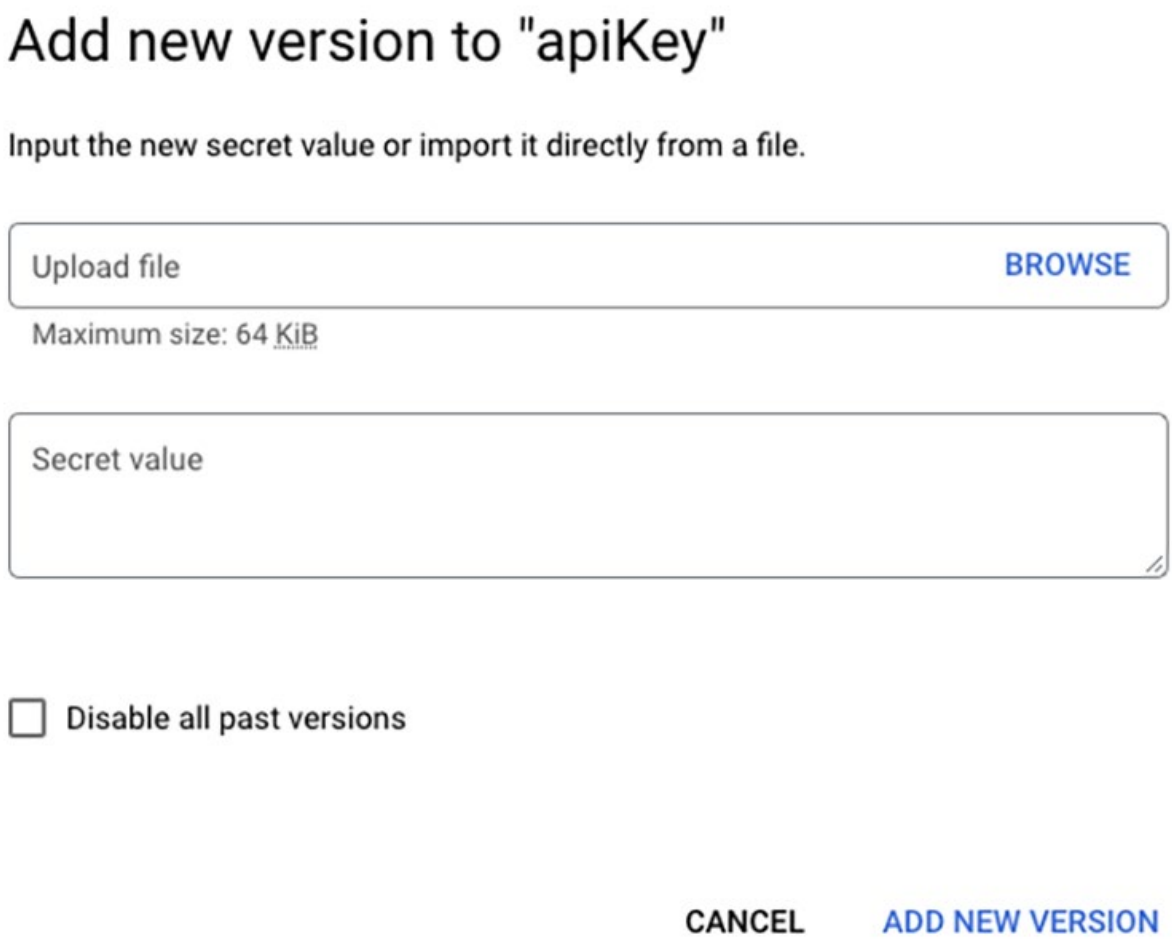


Figure 11.4 – Adding a new secret version (continued)

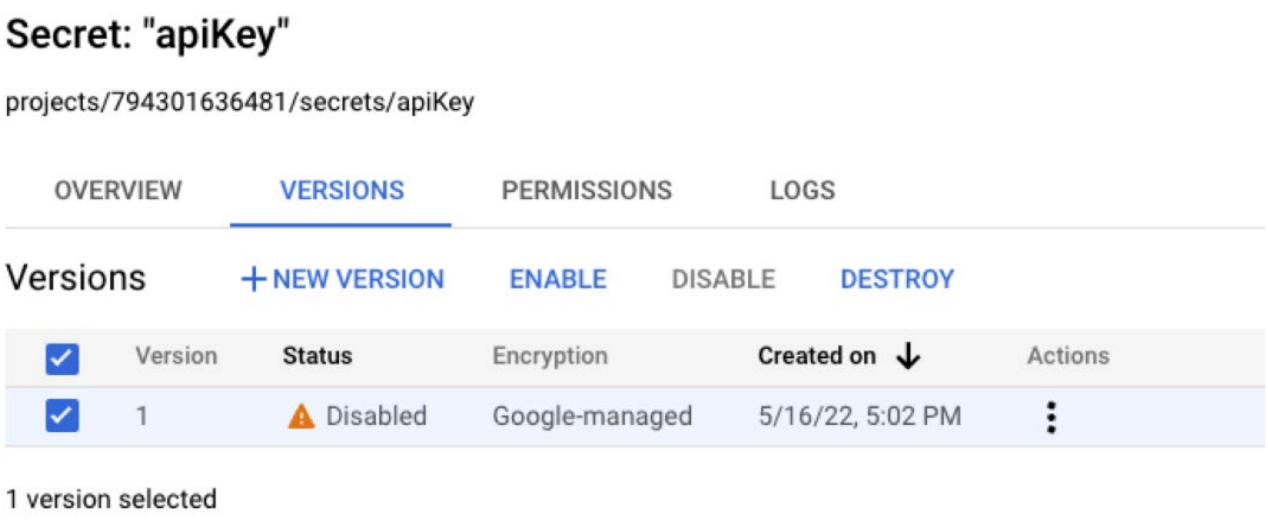


Figure 11.5 – Disabling a secret

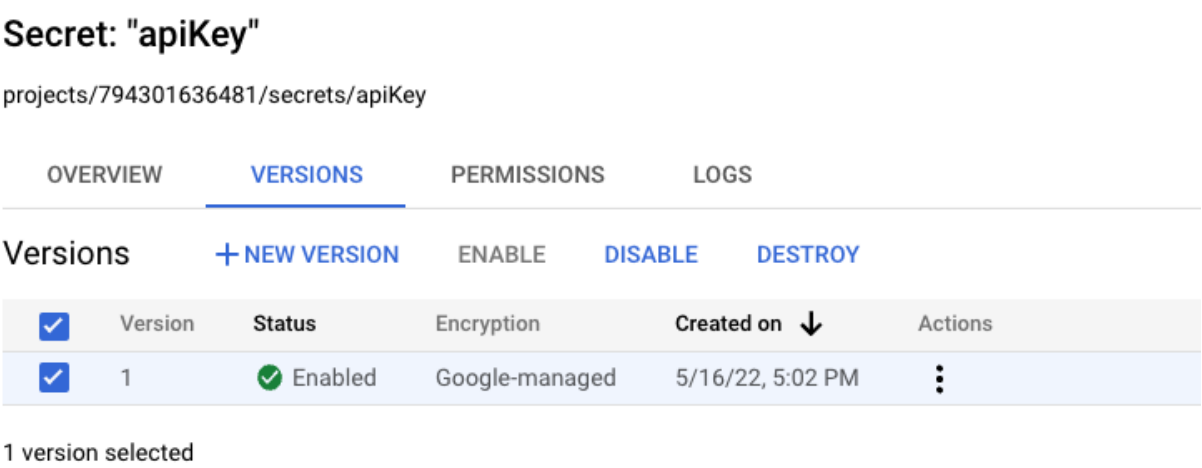


Figure 11.6 – Enabling a secret

Chapter 12: Cloud Logging

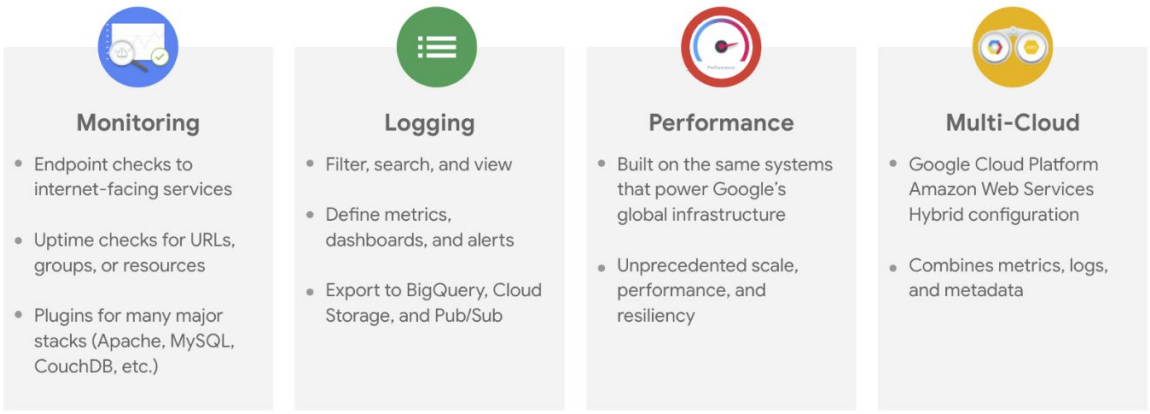


Figure 12.1 – Google Cloud's operations suite

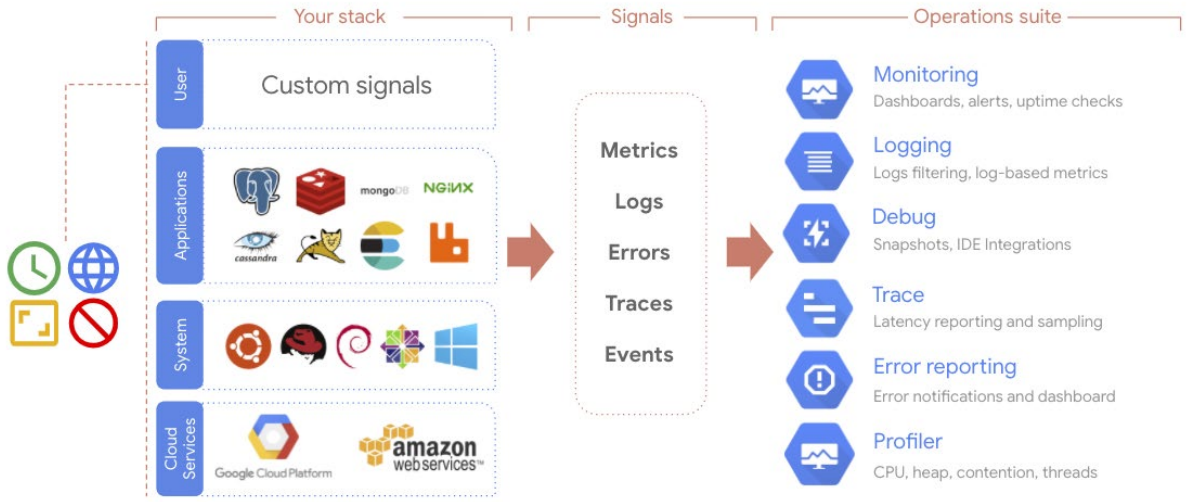


Figure 12.2 – Operations suite layers

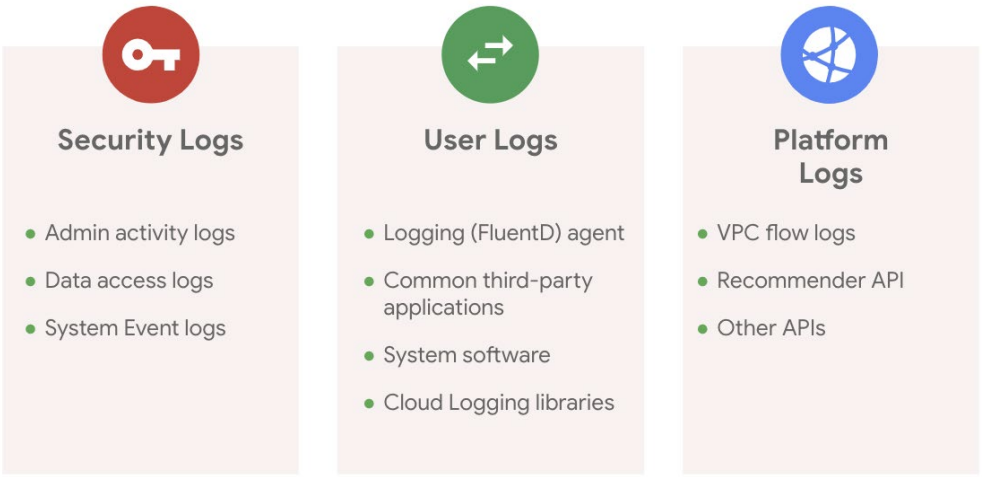


Figure 12.3 – Log categories

	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

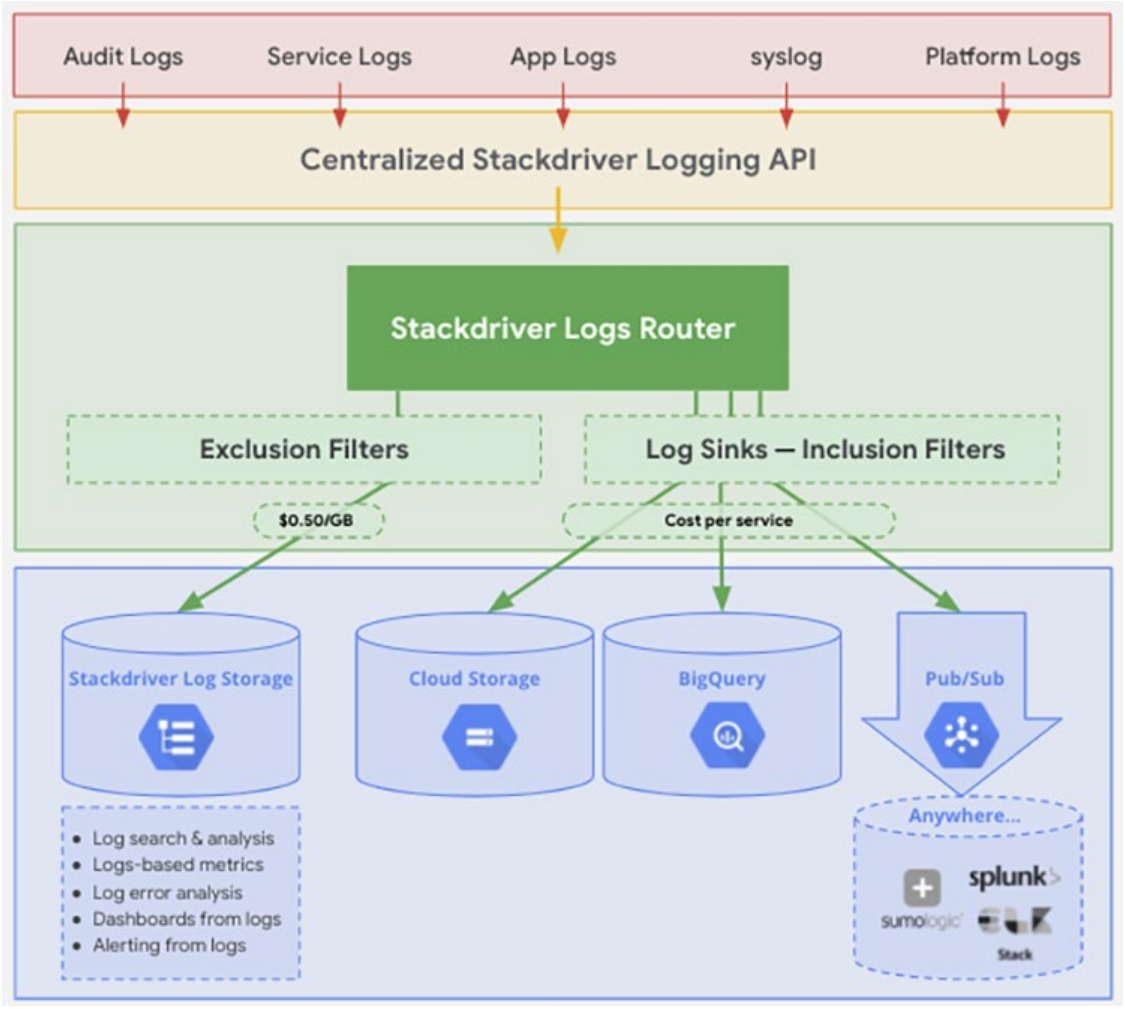


Figure 12.5 – Log Router

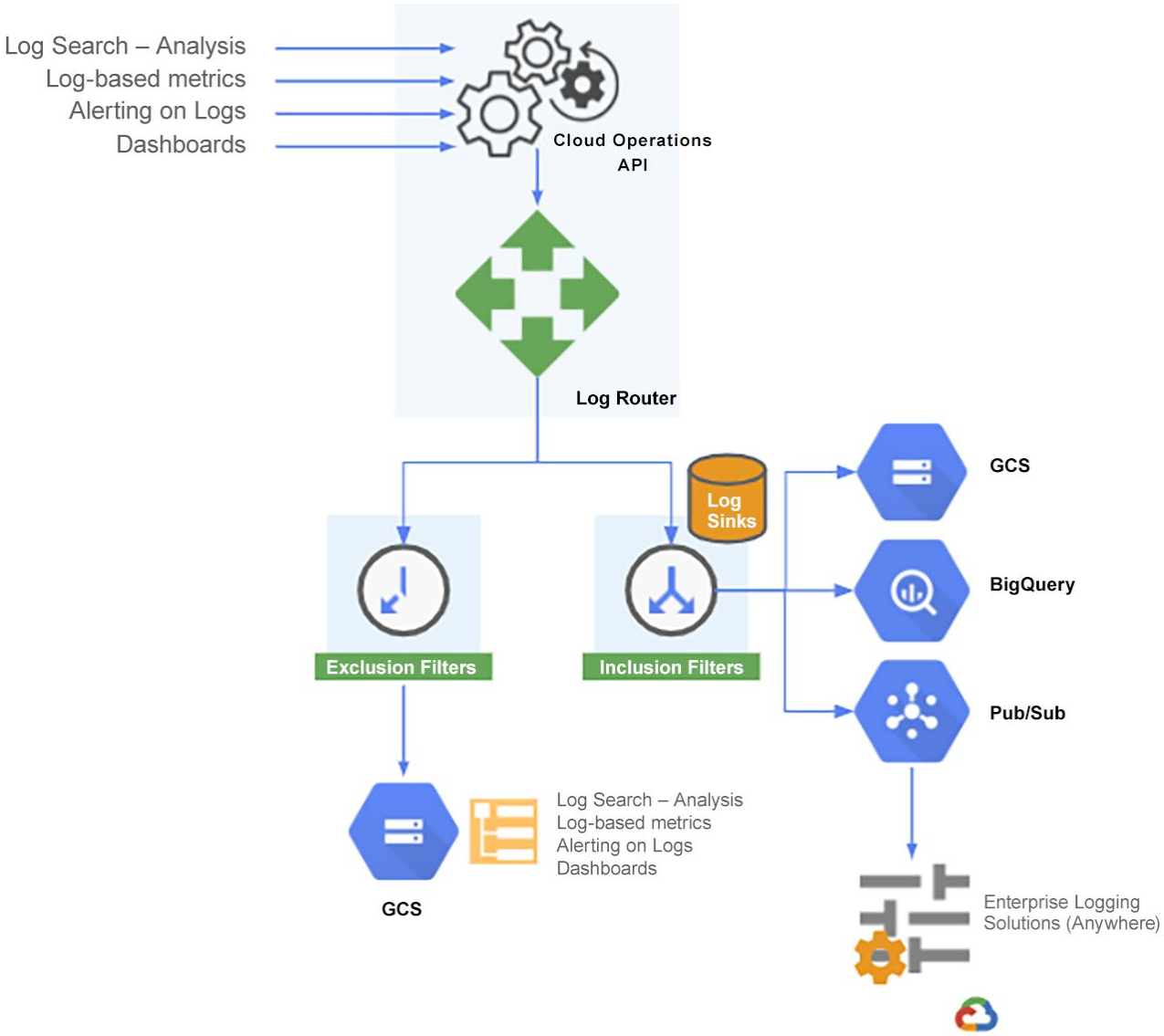


Figure 12.6 – Log exports and sinks

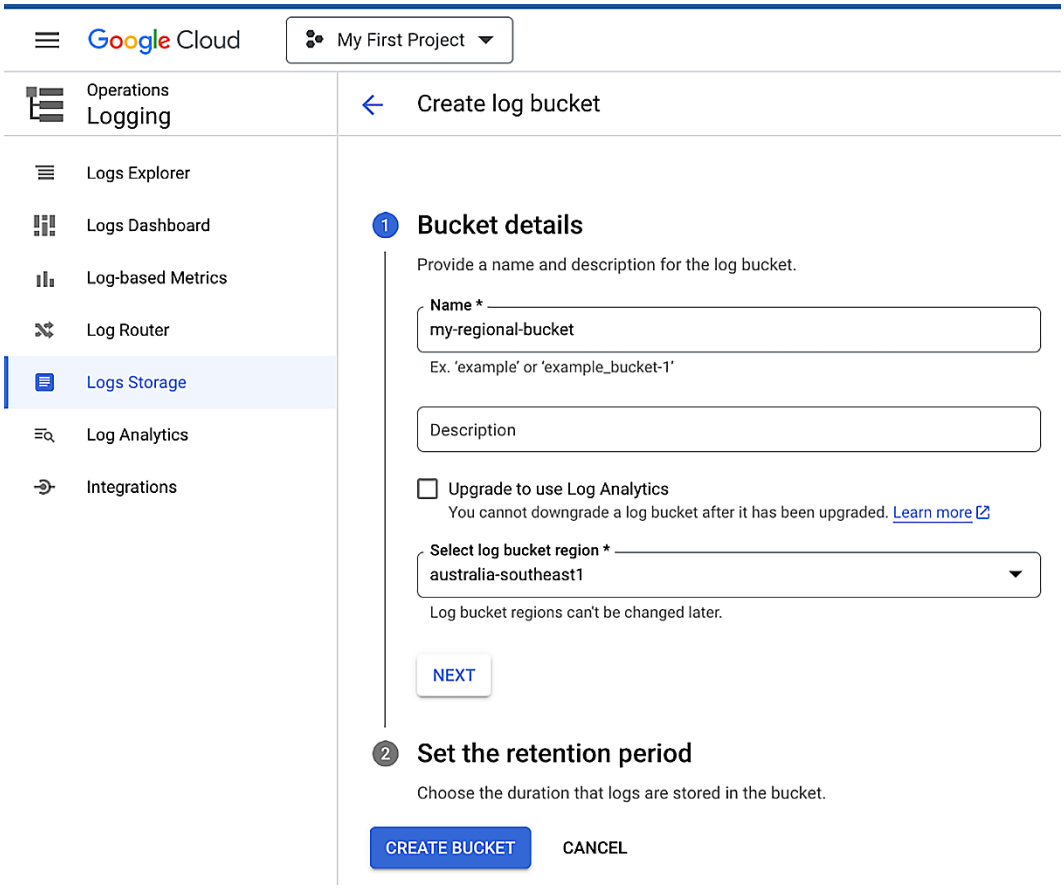


Figure 12.7 – Create log bucket

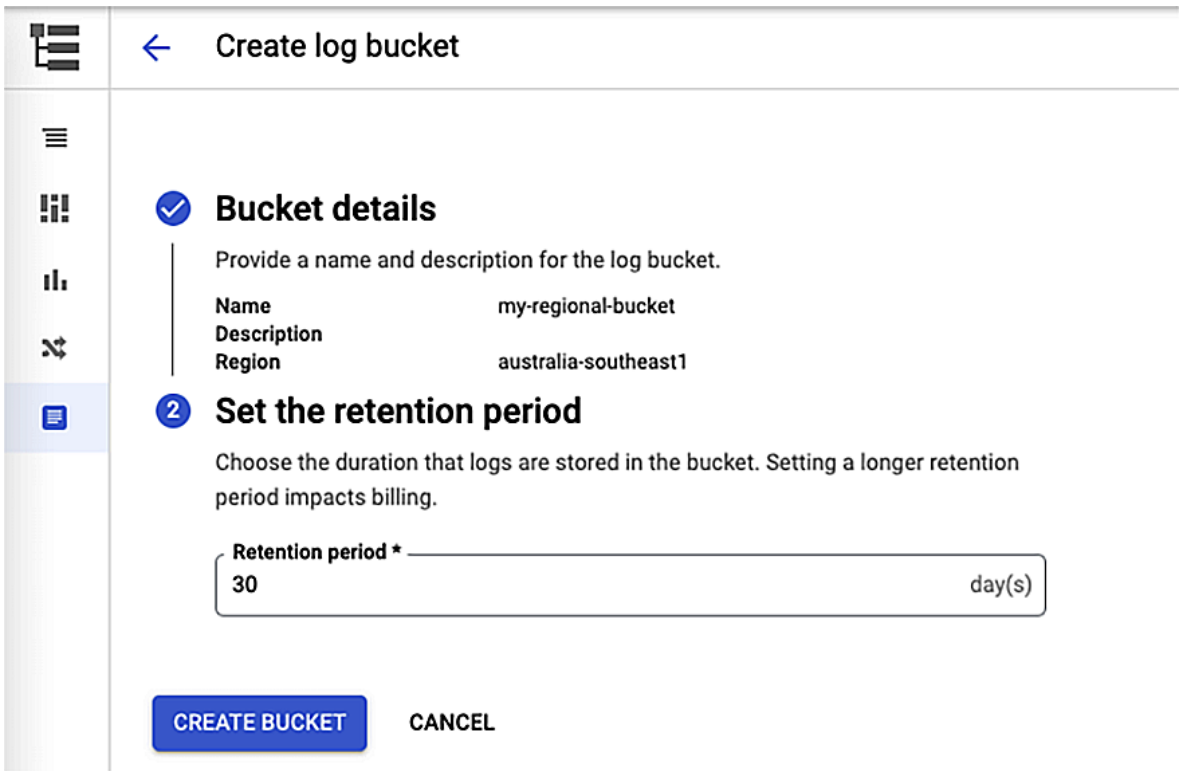


Figure 12.8 – Set the retention period for the log bucket

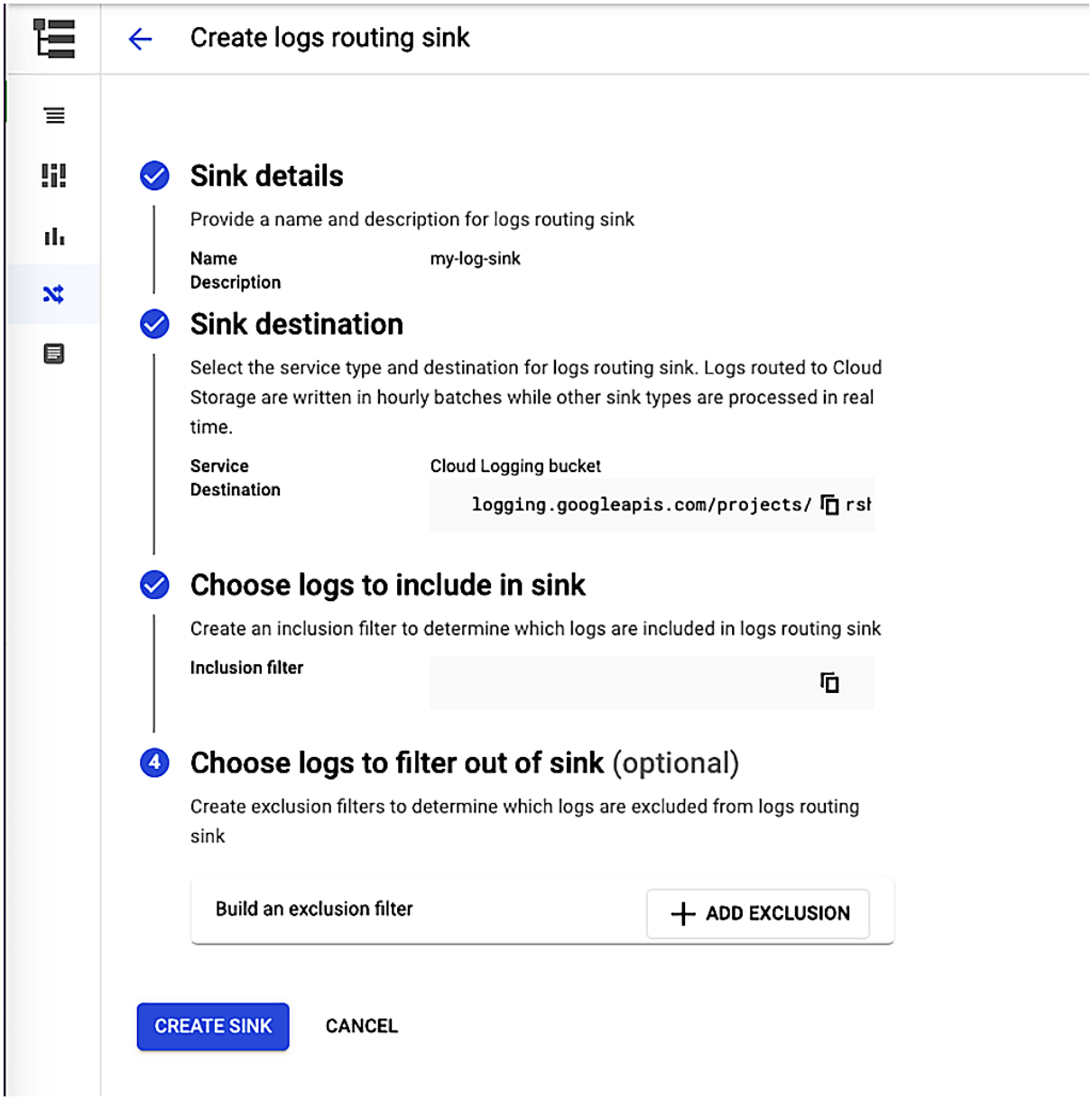


Figure 12.9 – Create a log sink

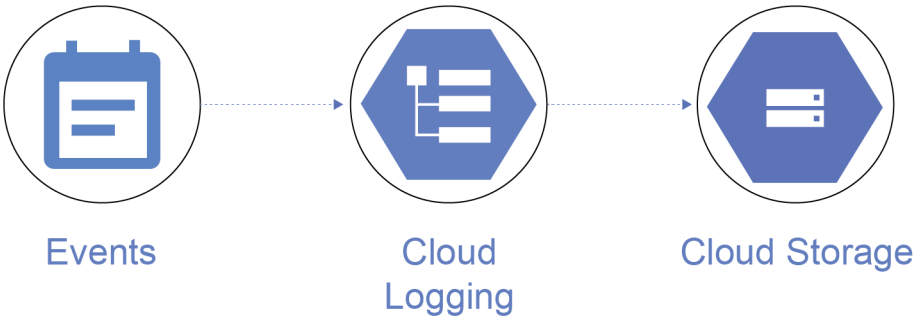


Figure 12.10 – Log archiving pipeline

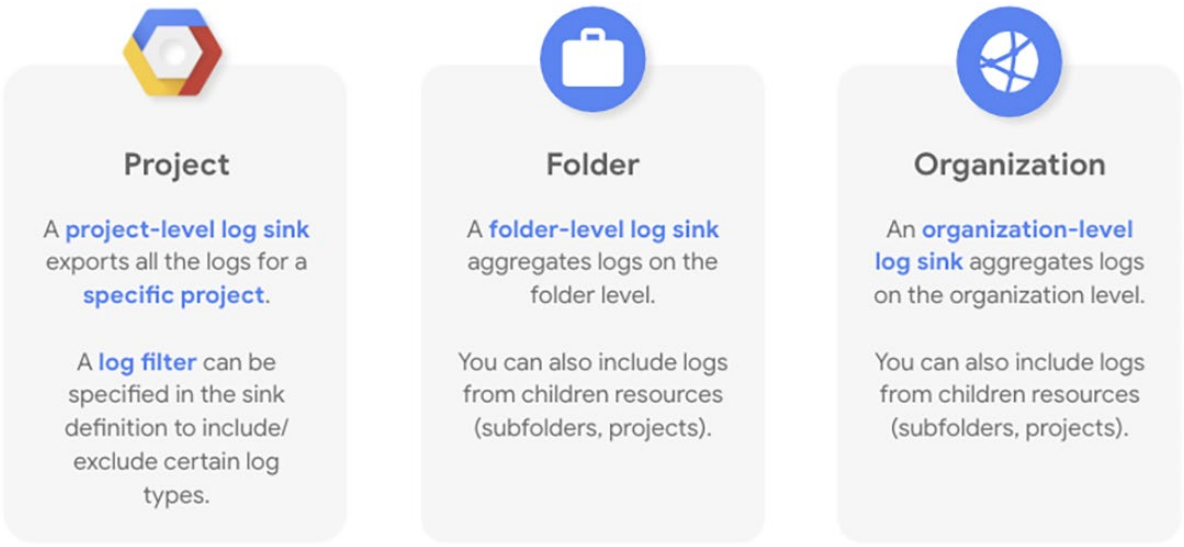


Figure 12.11 – Log aggregation

Figure 12.12 – Log streaming pipeline

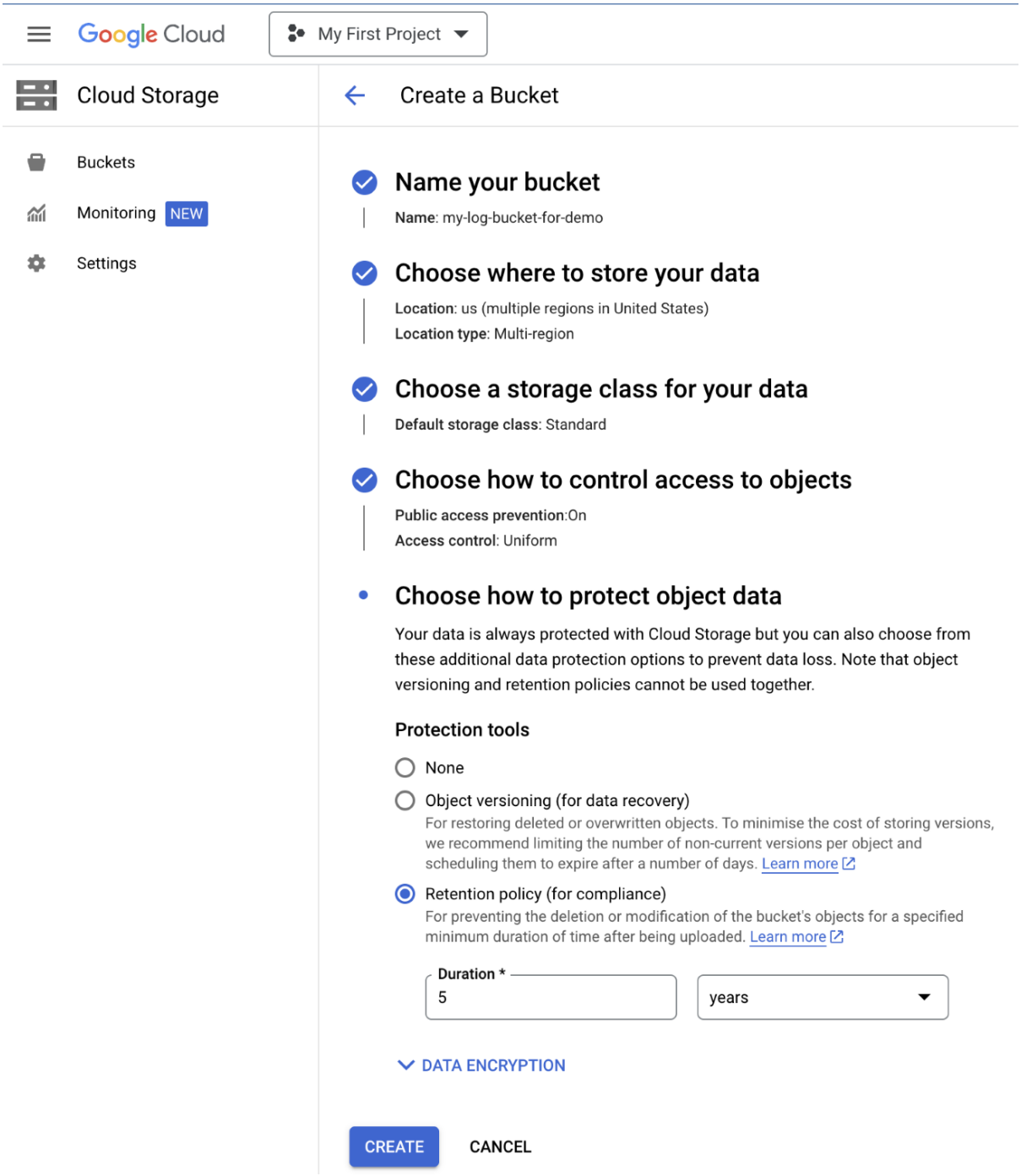


Figure 12.13 – Create a Cloud Storage bucket for logs

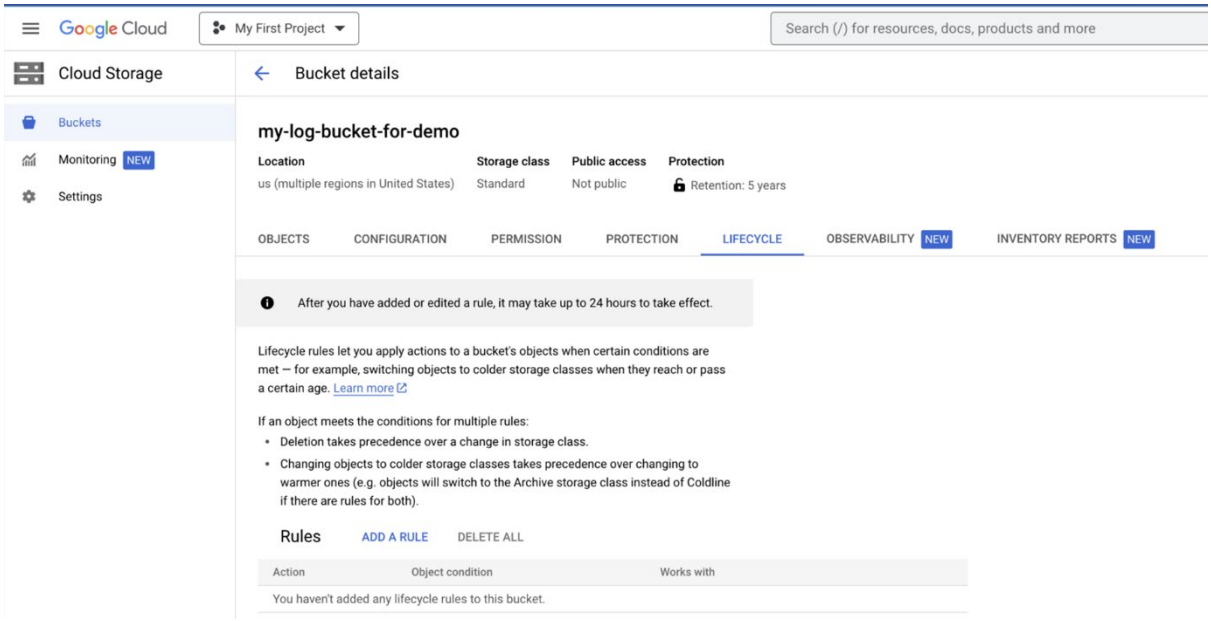


Figure 12.14 – The LIFECYCLE tab

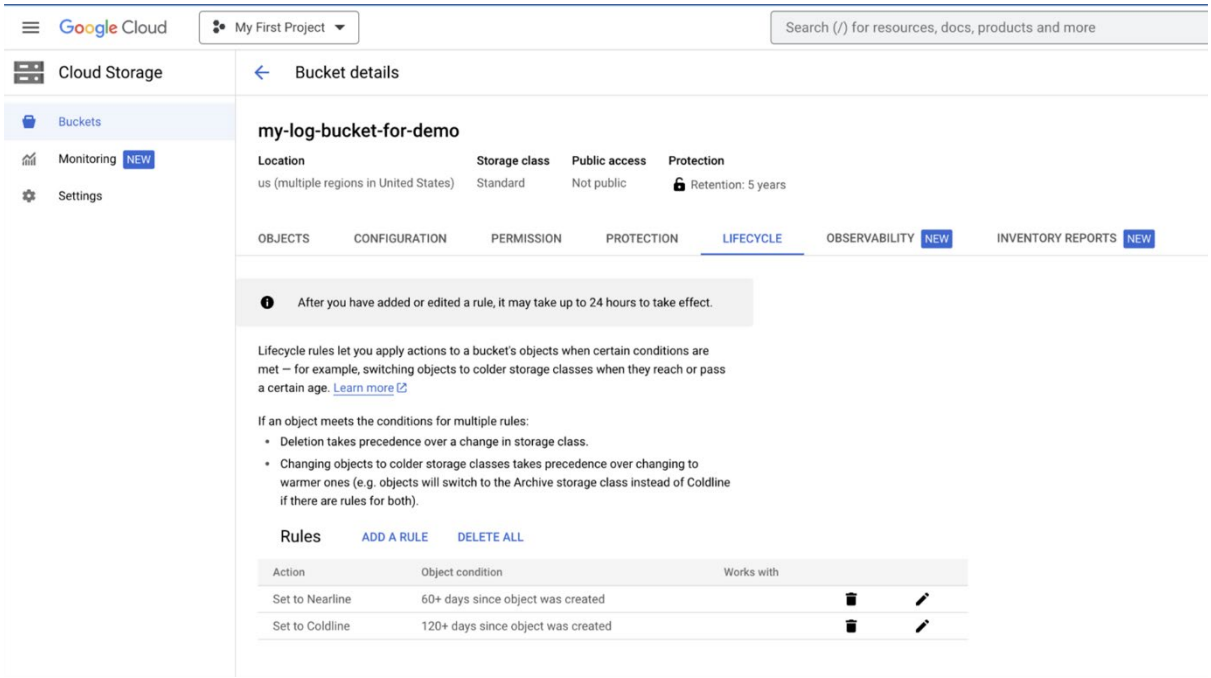


Figure 12.15 – Add a rule for lifecycle management

Chapter 13: Image Hardening and CI/CD Security

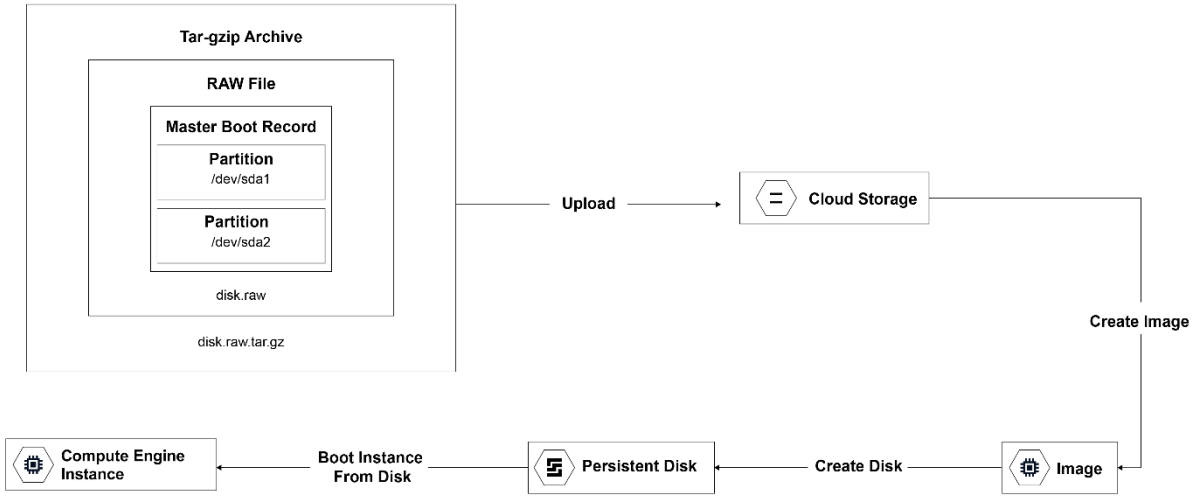


Figure 13.1 – A pipeline for creating a VM image

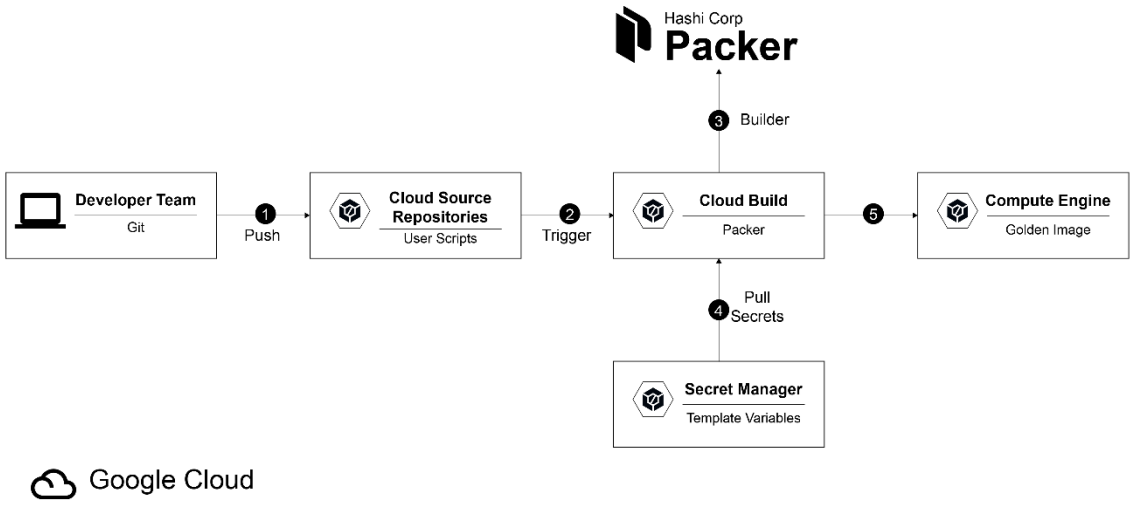


Figure 13.2 – VM image creation using Packer

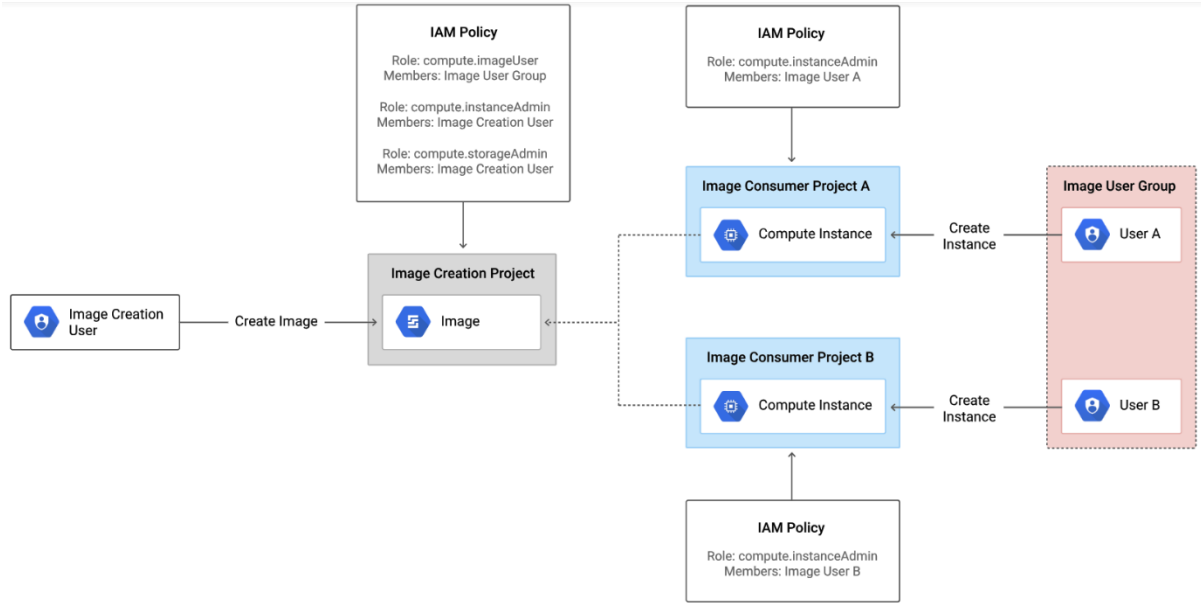


Figure 13.3 – Sharing images between projects

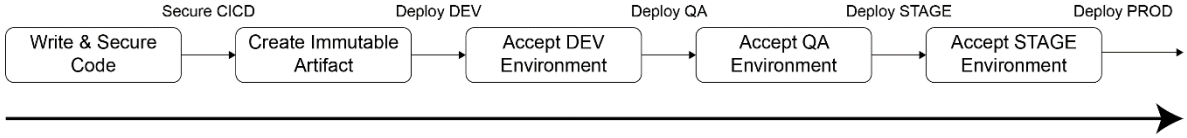


Figure 13.4 – Artifact trust

Chapter 14: Security Command Center

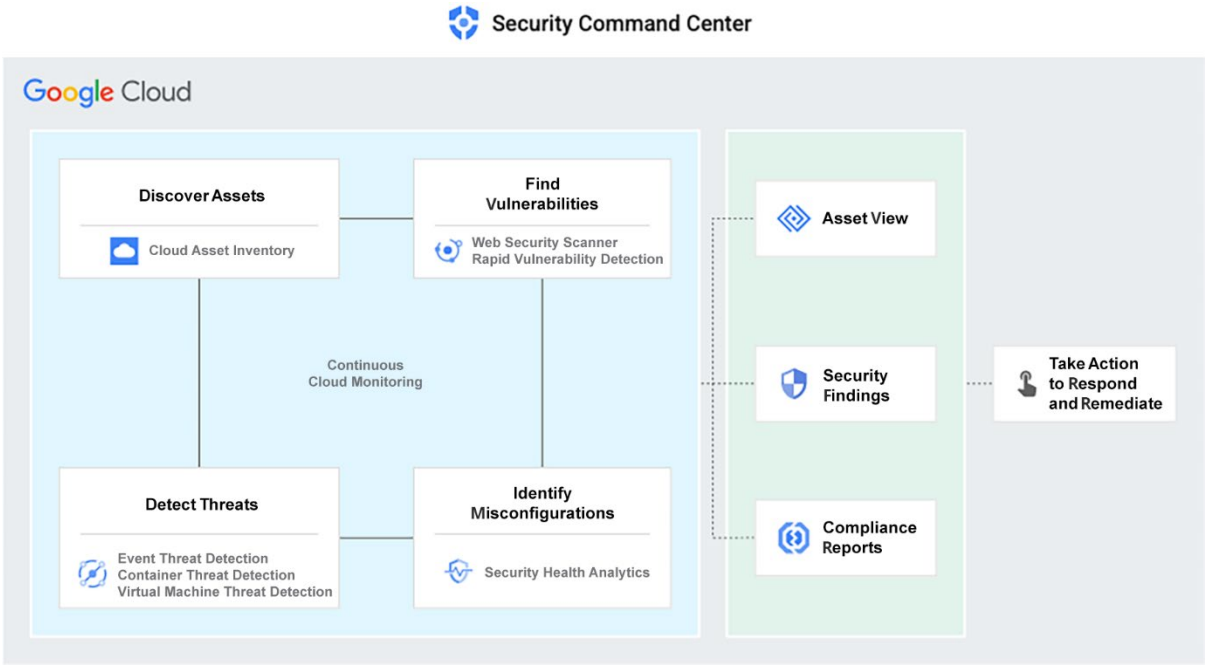


Figure 14.1 – SCC core services

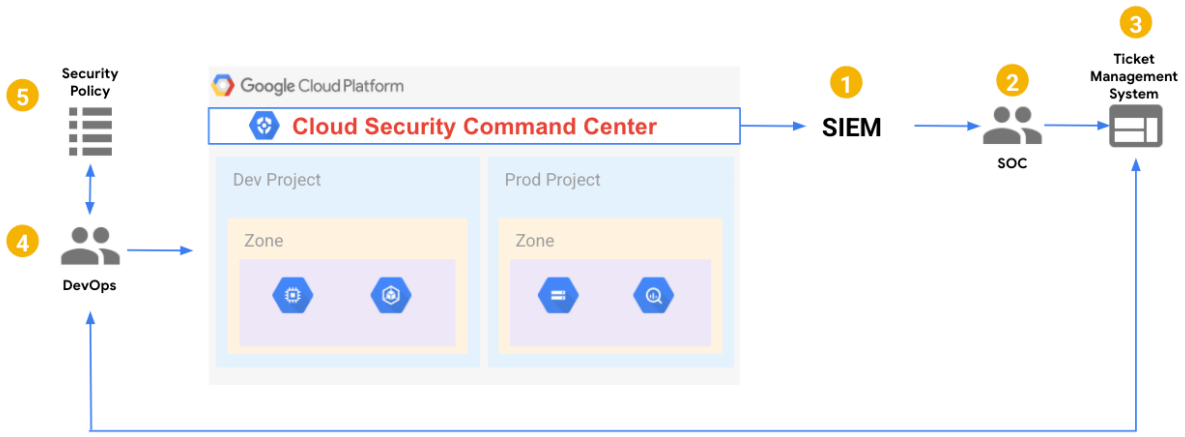


Figure 14.2 – Automating SCC response

Chapter 15: Container Security

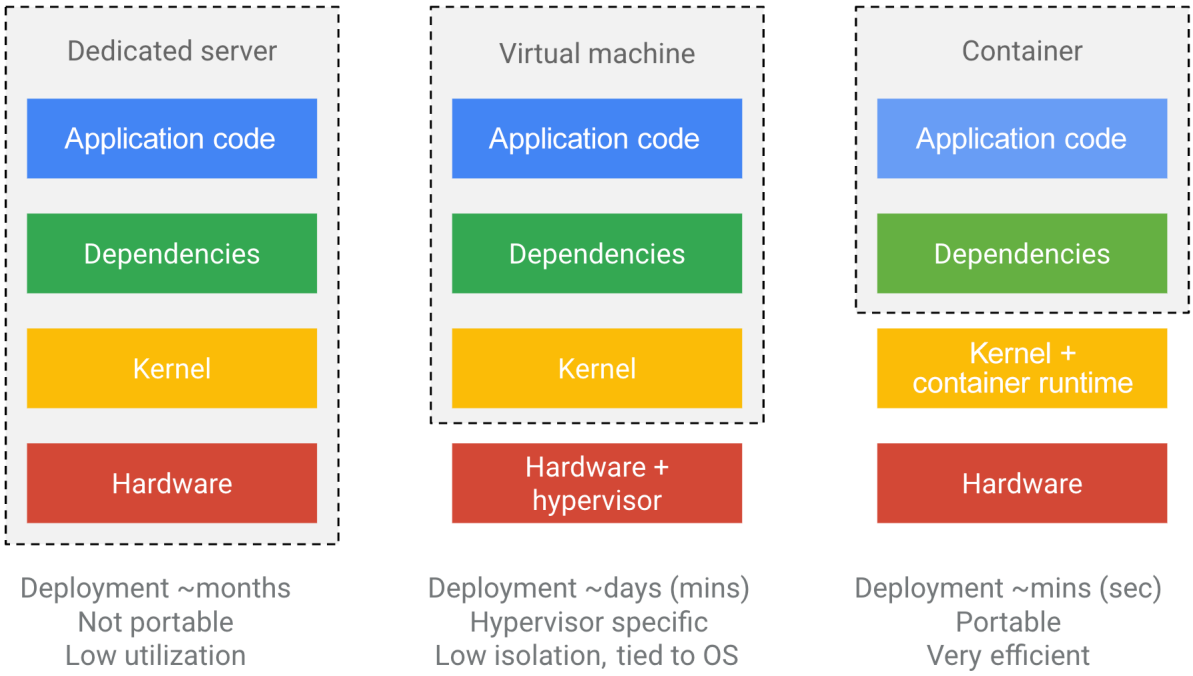


Figure 15.1 – Container structure

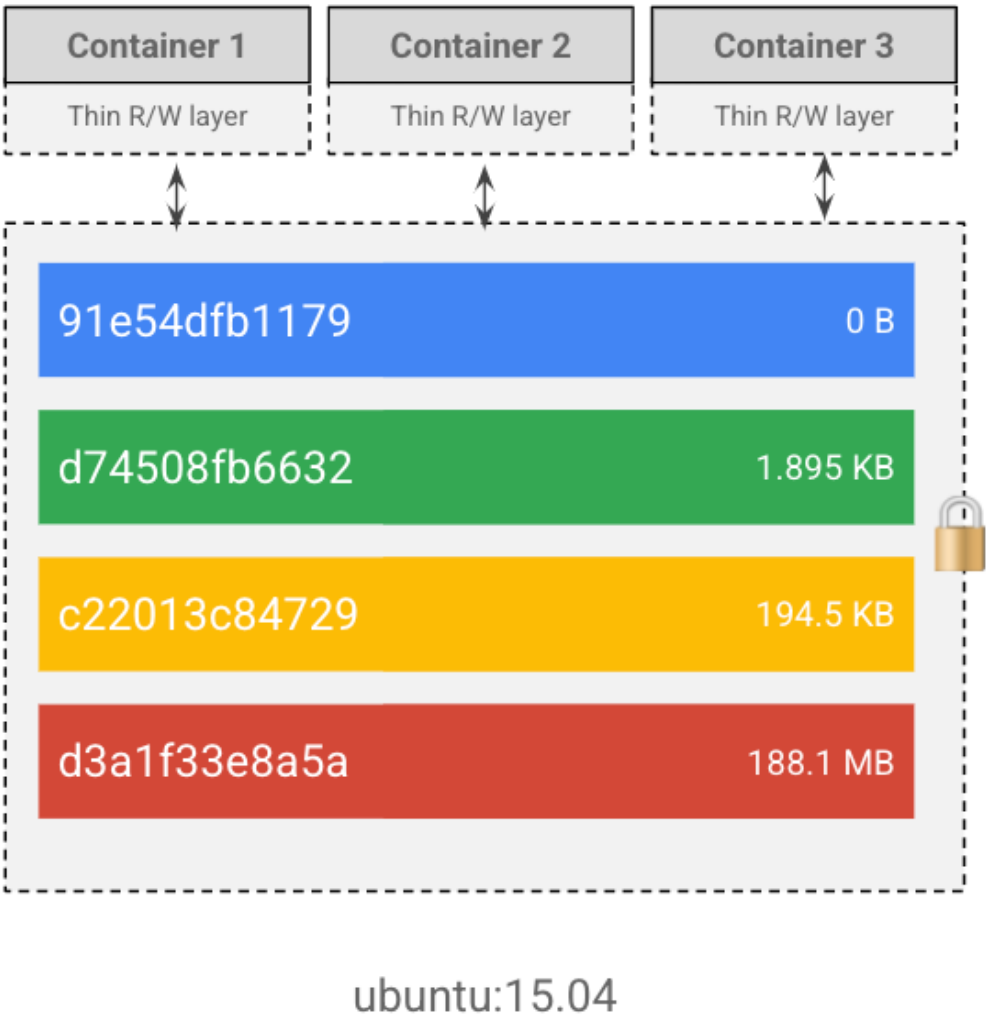


Figure 15.2 – Container layers

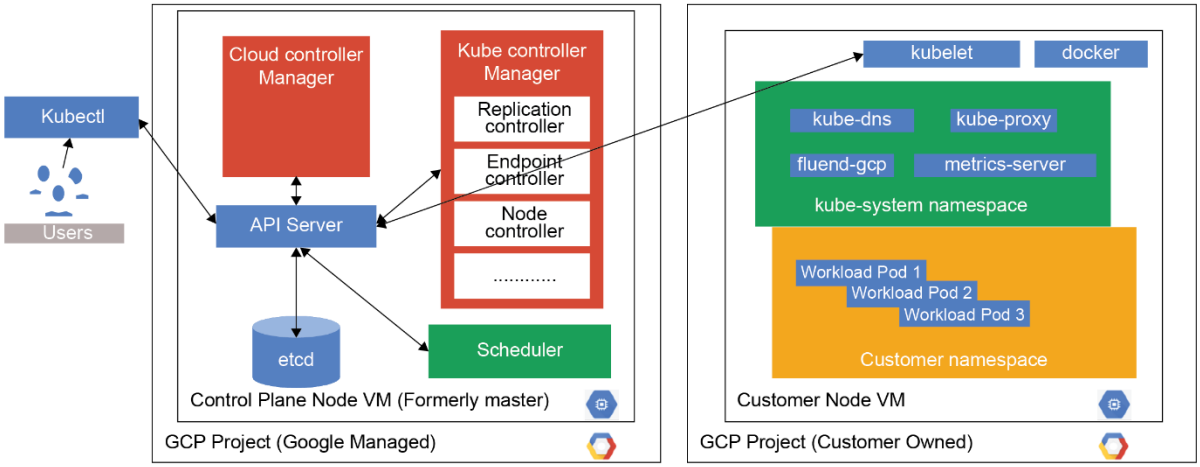


Figure 15.3 – GKE architecture

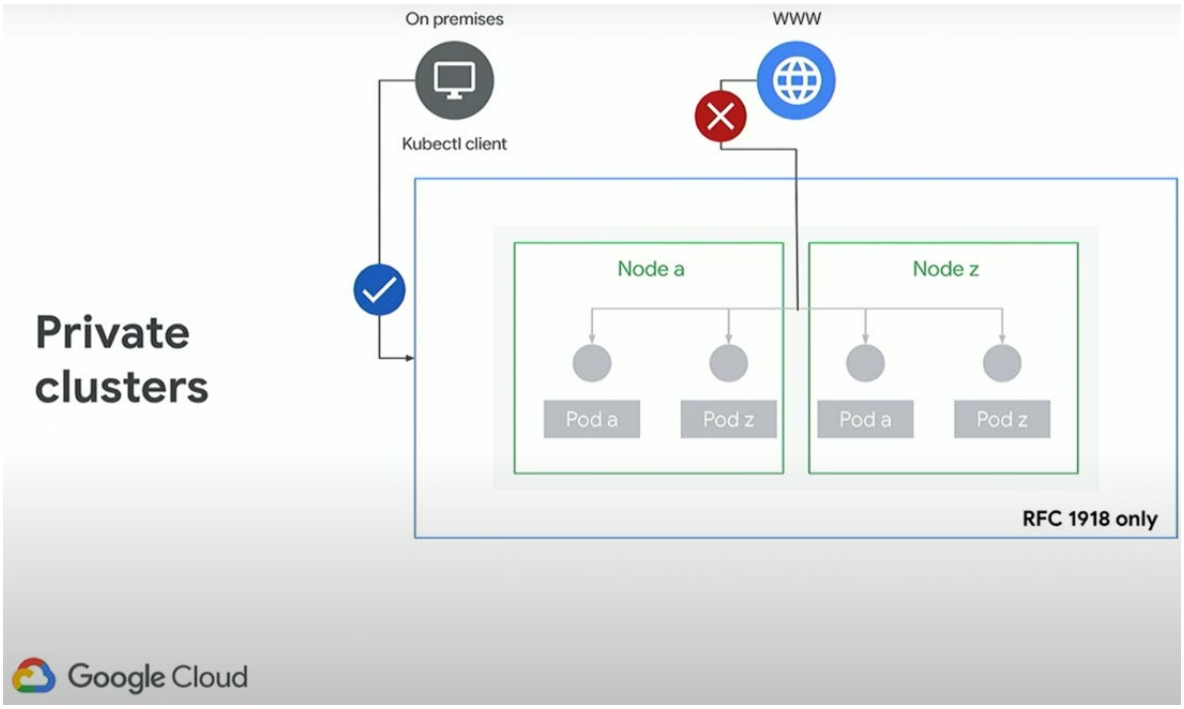


Figure 15.4 – Private clusters

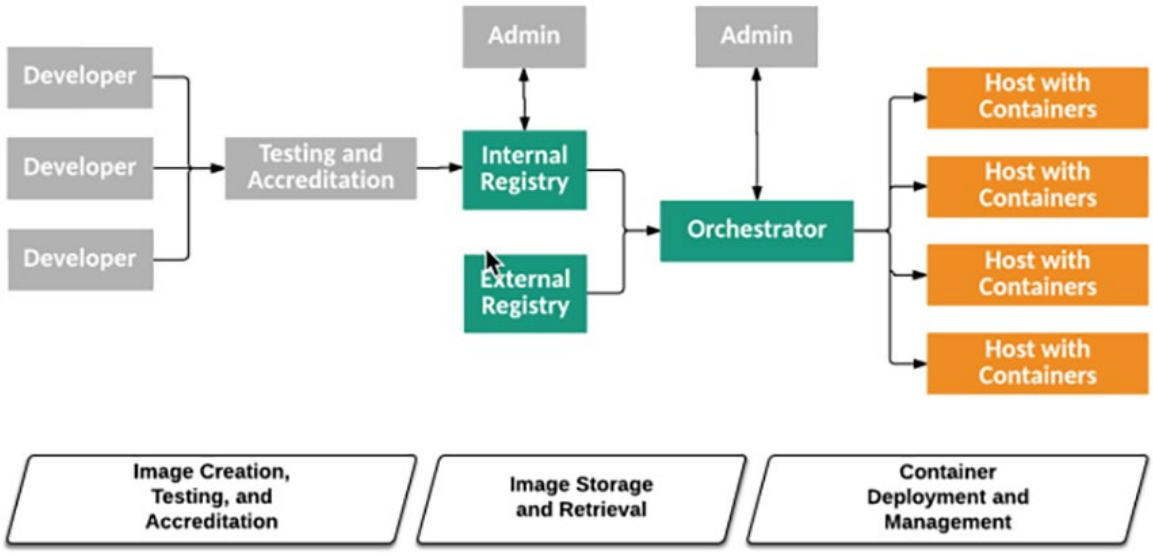


Figure 15.5 – Container pipeline

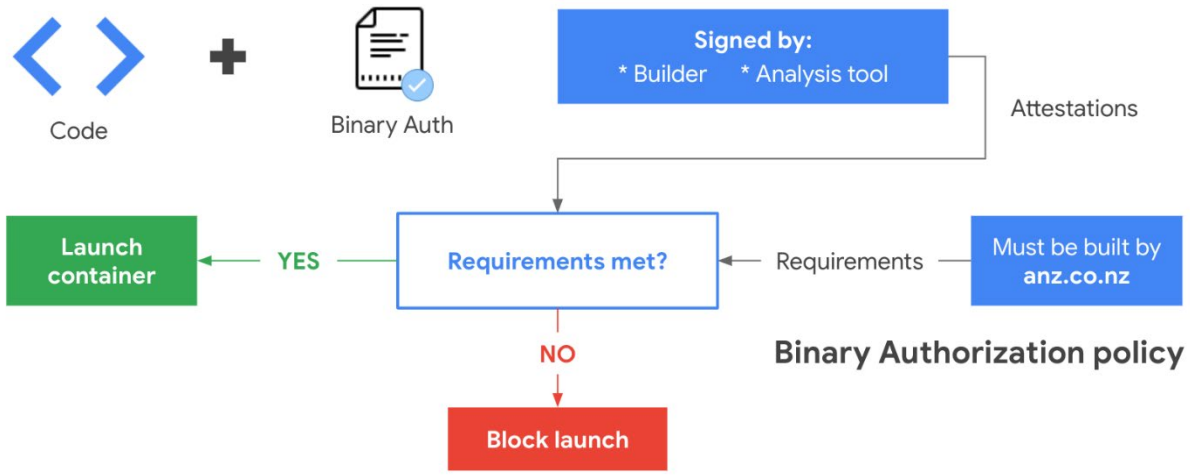


Figure 15.6 – Binary Authorization

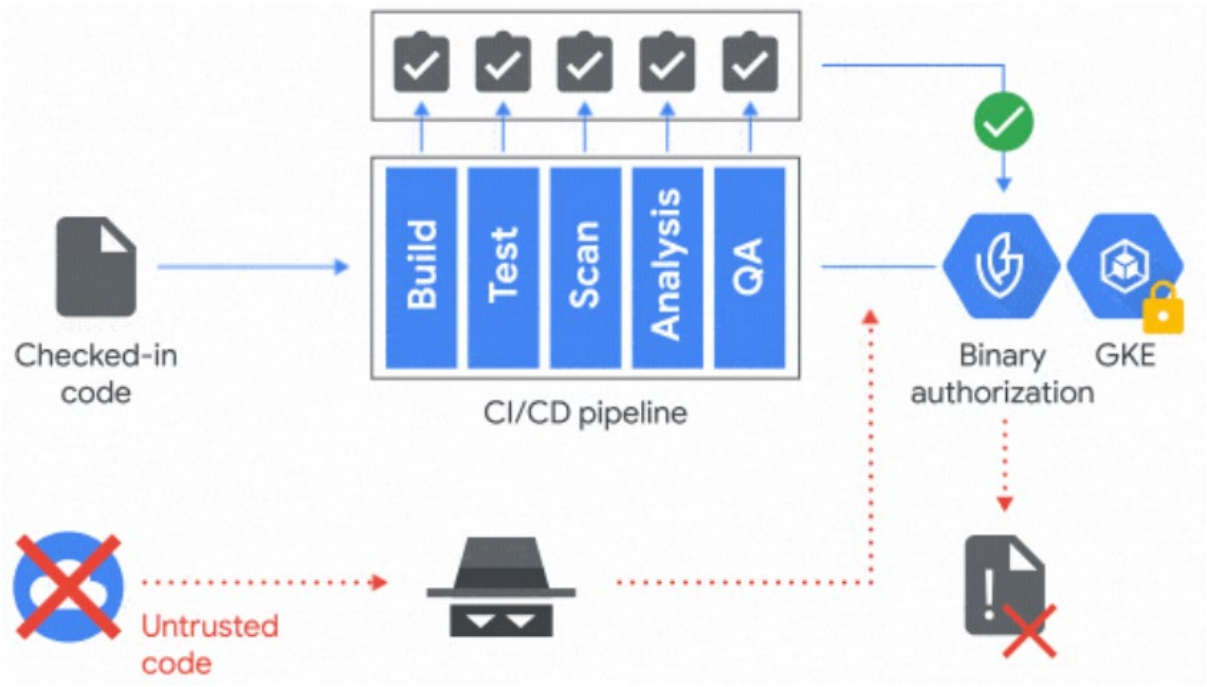


Figure 15.7 – Binary Authorization in the CI/CD pipeline