SCOPE: ~23% of Exam Syllabus

Architecting Data Protection in Google Cloud

```
provider "google" {
  project = var.project_id
  region  = var.region
}
```

Decoding Section 3 of the PSE Exam into Production-Ready Terraform

Stage 1: The Edge

Isolating the Network

app_networking | Private IPs

Stage 2: The Application

Securing Secrets

app_secrets | Rotation & Injection

Stage 3: The Core

Cryptographic Control

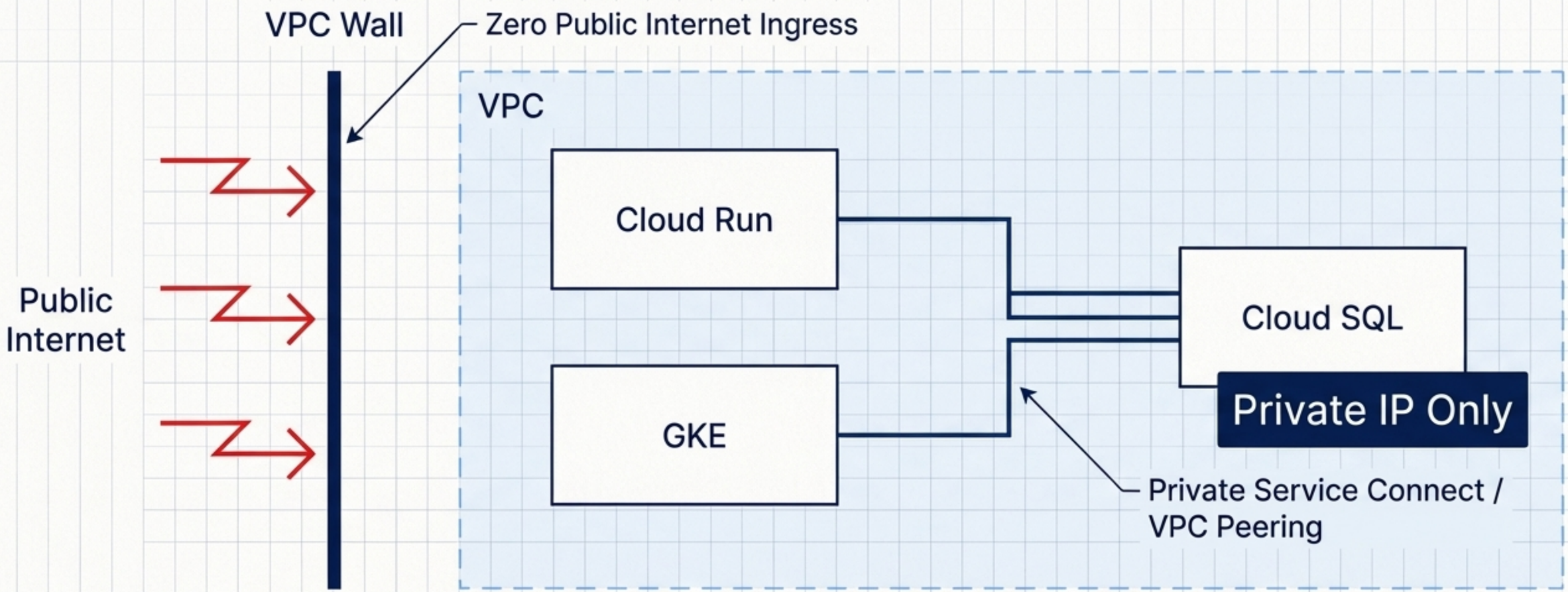
cmek.tf | Default vs. CMEK

Stage 4: The Lifecycle

Enforcing Privacy

app_storage_wrapper | Retention Policies

The Private Service Connect Anatomy




```
Location: modules/App_GCP/modules/app_networking/main.tf
Action: Restricts Cloud SQL access to authorized internal compute resources.
```

```
modules/
  App_GCP/
    modules/
      app_secrets/
        main.tf
```

Step 1

random_password.database_password

(Generates raw string)

Step 2

google_secret_manager_secret

Step 3

Application Environment

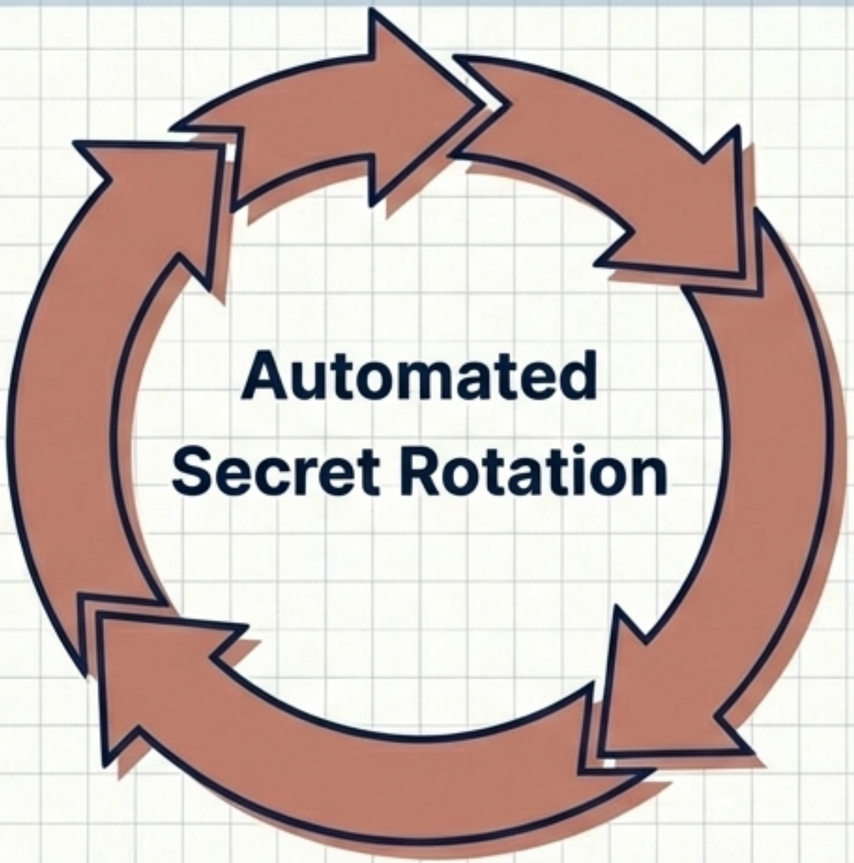
(Cloud Run/GKE)

Infrastructure-as-Code provisions secure generation, storage, and injection of database passwords, Redis auth strings, and application keys.

Secrets are dynamically rotated via Pub/Sub topics, ensuring long-lived infrastructure does not rely on static credentials.

Trigger

`google_pubsub_topic.secret_rotation`



Execute

Cloud Function/Compute authorized to rotate

Update

`google_secret_manager_secret_version` writes the new value

Propagate

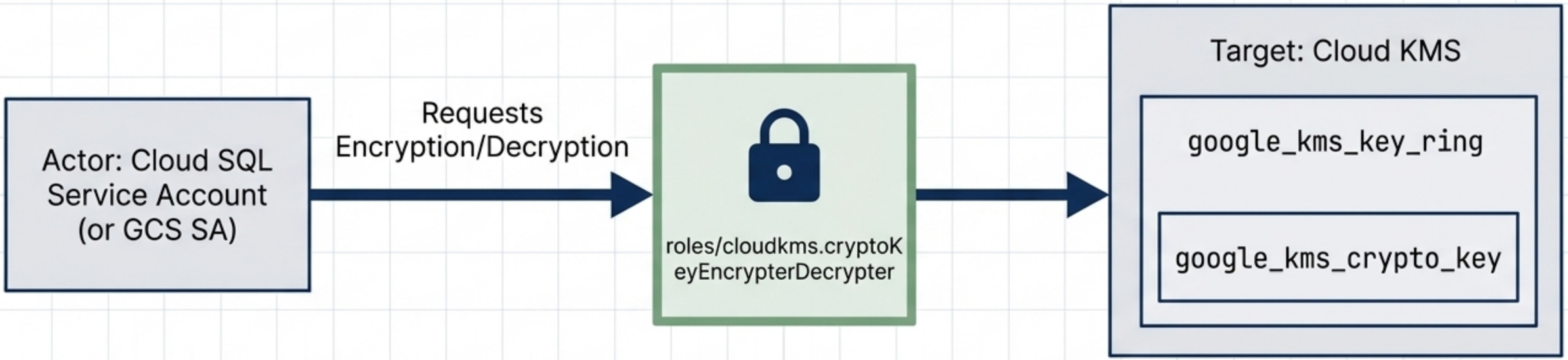
New secret injected into Application compute environment

The Encryption Responsibilty Matrix

	Default Encryption (At Rest)	CMEK (At Rest)	SSL/TLS (In Transit)
Locus of Control	Google-Managed	Customer-Managed	Edge Terminated
Key Manager	Internal Google Systems	Cloud KMS (`google_kms_crypto_key`)	Managed Certificates
Target Services	All storage by default	Cloud SQL, Artifact Registry, GCS	Load Balancers
Terraform Path	N/A (Default)	modules/Services_GCP/cmek.tf	Networking/LB configs

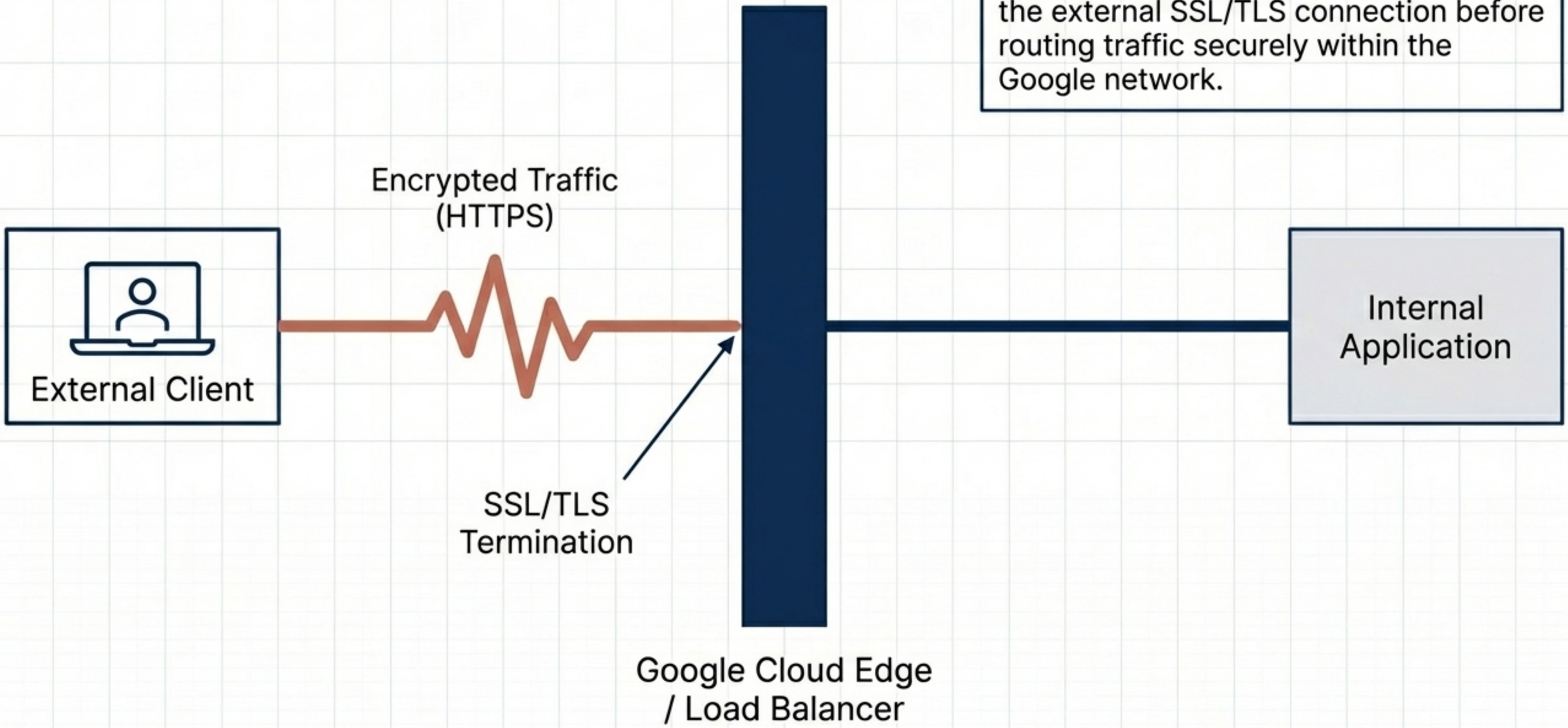
Exam Rule: Identify who controls the keys and where encryption is applied.

The CMEK Delegation Model

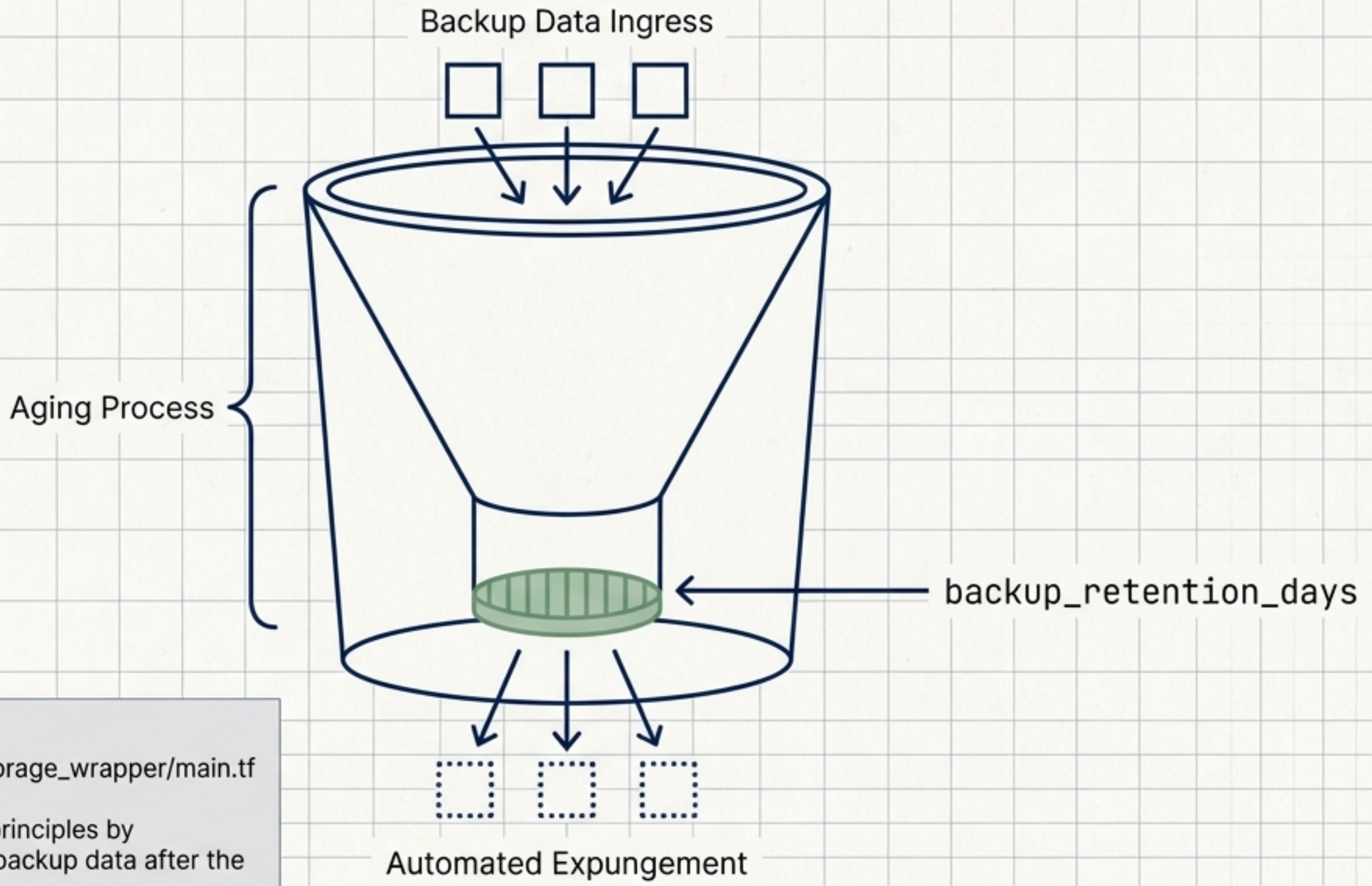


Location: modules/Services_GCP/cmek.tf
Requirement: Services must be explicitly granted KMS permissions to utilize customer-managed keys.

Encryption in transit is enforced at the edge. The Load Balancer terminates the external SSL/TLS connection before routing traffic securely within the Google network.



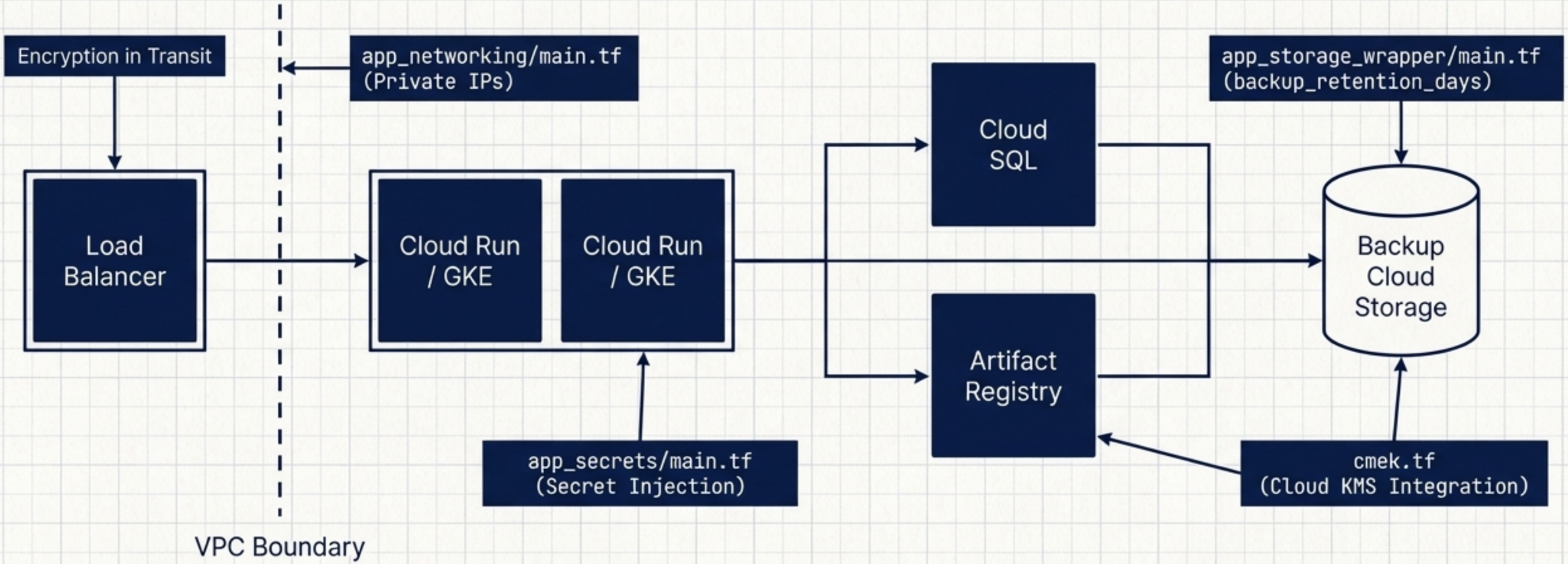
The Data Privacy Funnel



Location:
modules/App_GCP/modules/app_storage_wrapper/main.tf

Mechanism: Enforces data privacy principles by automatically cleaning up sensitive backup data after the defined retention period.

The Master Architecture Overlay



Section 3 Mastery: Data protection is not a single service—it is a continuous, layered architecture codified directly into your Terraform configuration.