Google Cloud

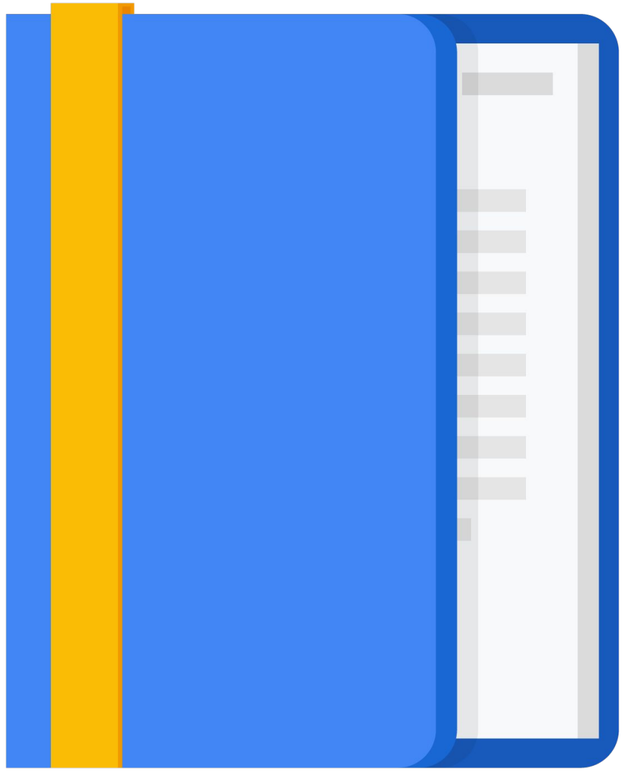
Security

Learning objectives

- Design secure systems using best practices like separation of concerns, principle of least privilege, and regular audits.
- Leverage Google's Security Command Center to help identify vulnerabilities.
- Simplify cloud governance using organization policies and folders.
- Authenticate and authorize users with IAM roles, Identity-Aware Proxy, and Identity Platform.
- Manage the access and authorization of resources by machines and processes using service accounts.
- Secure networks with private IPs, firewalls, and Google Cloud private access.
- Mitigate DDoS attacks by leveraging Cloud DNS and Google Cloud Armor.

Agenda

- Security Concepts
- Securing People
- Securing Machine Access
- Network Security
- Encryption
- Design Activity #12



Google Cloud security is a shared responsibility between you and Google

Transparency

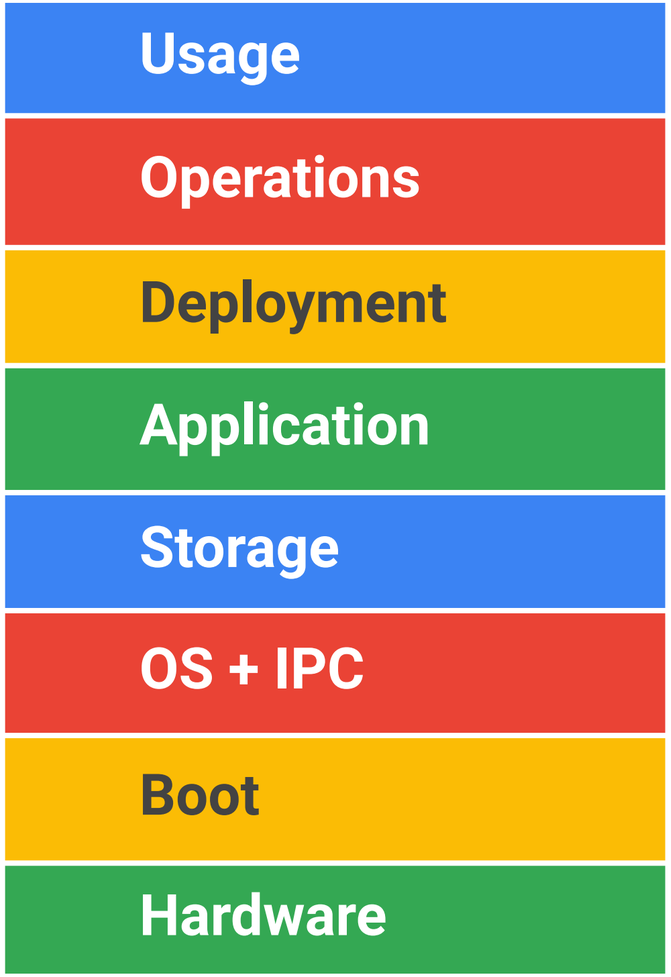
- The client is responsible for certain actions, and Google is responsible for others.
- Google Cloud provides the tools and access to monitor your service.
- Google Cloud provides the controls and features needed to leverage platform security.

Separation of duties

- What is provided by the platform?
- What are you responsible for?

Security is implemented in layers

- Google Cloud provides tools that, when properly configured, enable a secure environment.
- You can also integrate third-party tools for enhanced security.
- There are tools for monitoring and auditing your networks and resources.



Principle of least privilege

- Users should only be able to do the tasks that are required by their jobs.
- This should also apply to machine instances and run-time processes.

- Use IAM to enforce this principle.
- Identify users with their login.
- Identify machines and code using service accounts.
- Assign IAM roles to users and service accounts to restrict what they can do.

Separation of duties

Separation of duties means:

- No one person can change or delete data without being detected.
- No one person can steal sensitive data.
- No one person is in charge of designing, implementing, and reporting on sensitive systems.

For example, the people who write the code shouldn't deploy the code, and those who deploy the code shouldn't be able to change it.

- Use multiple projects to separate duties.
- Different people can be given different rights in different projects.
- Use folders to help organize projects.

Regularly audit the Google Cloud logs to discover attacks

All Google Cloud services write to audit logs:

- Admin logs
- Data access logs
- VPC Flow logs
- Firewall logs
- System logs

Google Cloud meets many third-party and government compliance standards worldwide

- Google Cloud has been certified as secure, but that does not mean that your application is certified.
- Don’t worry about getting Google Cloud tools and services certified; only worry about what you build on top of Google Cloud.

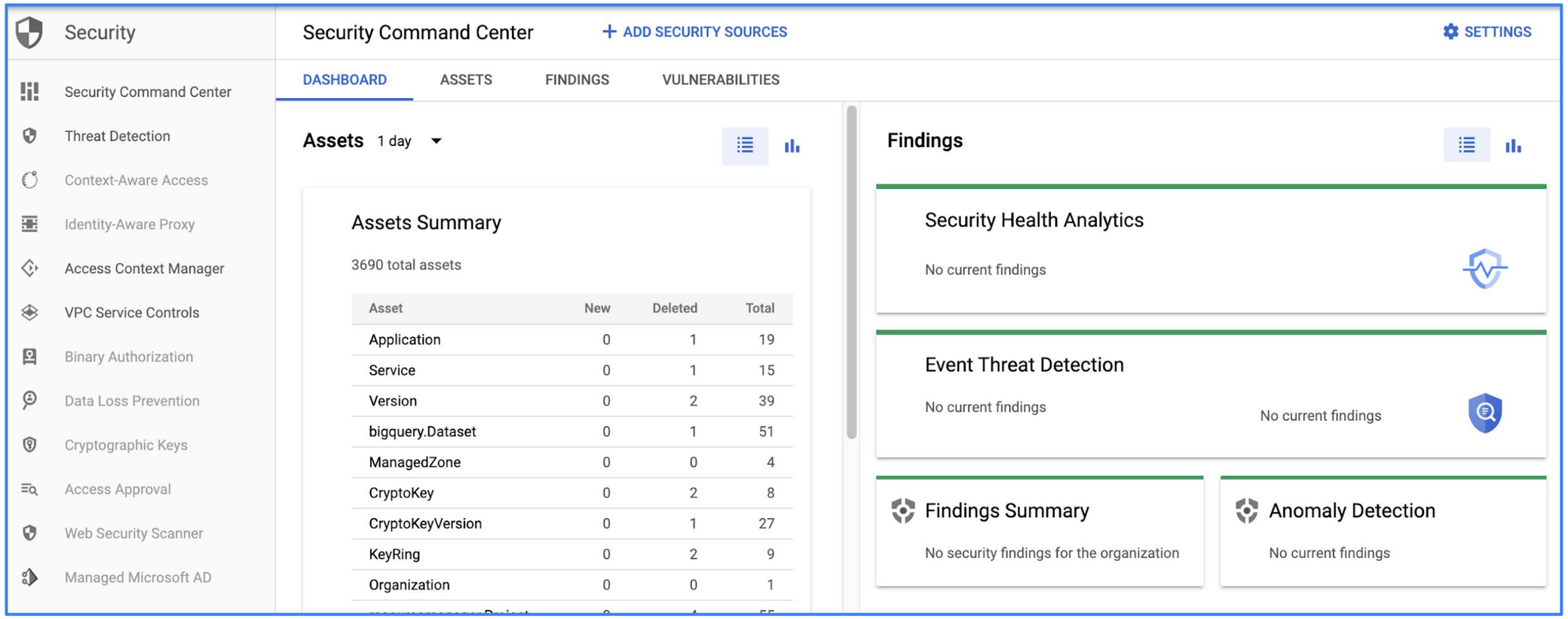
ISO/IEC 27001

HIPAA

FedRAMP

SOC 1

Security Command Center provides access to organizational and project security configuration



Google Cloud

Agenda

Security Concepts

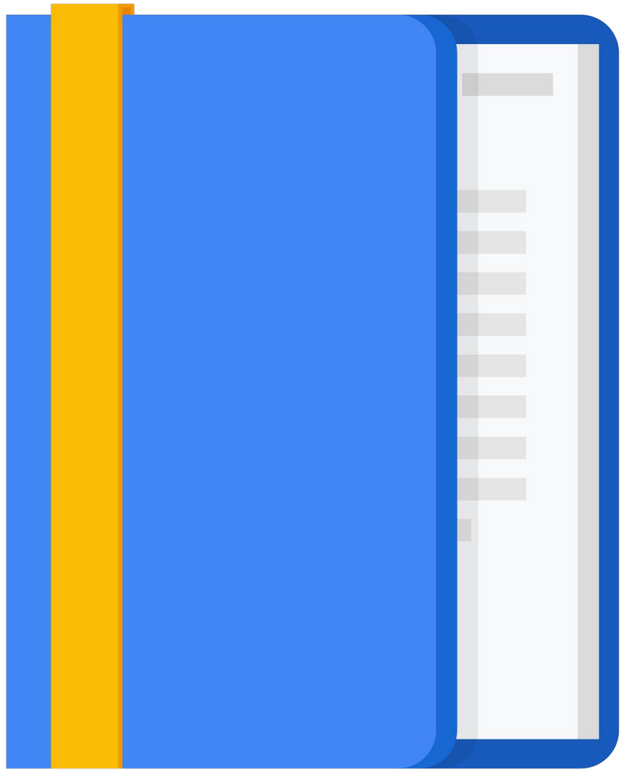
Securing People

Securing Machine Access

Network Security

Encryption

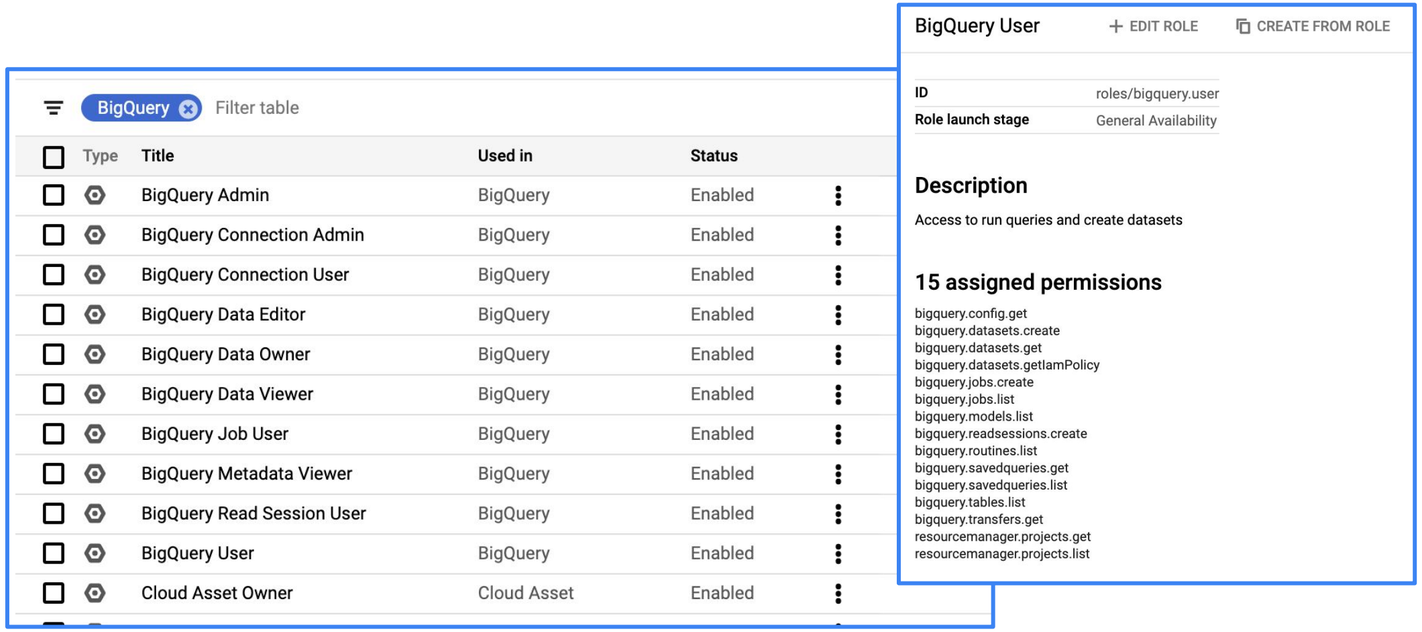
Design Activity #12



To grant people access to your projects, add them as members and assign them one or more roles

- Members are identified by their login.
- Add members to groups for easier management.

- Roles are simply a list of permissions.
- Use the Console to easily see what permissions are granted to roles.



Google Cloud

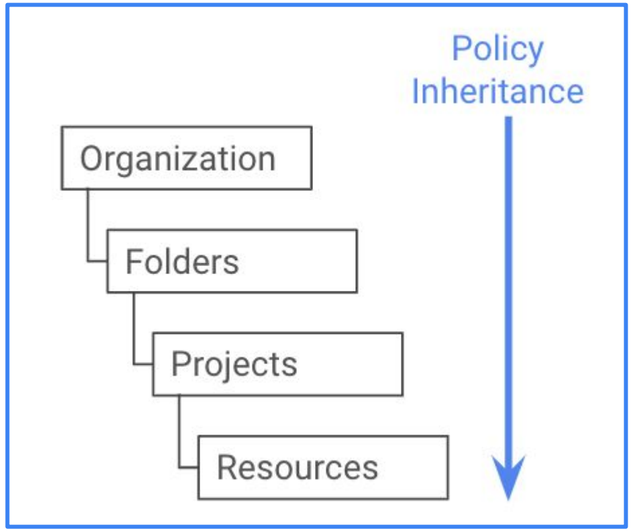
Use organizational policies and folders to simplify securing environments and managing resources

Grant roles to Google groups rather than individuals

- Groups can be more granular than job roles.
- Use multiple groups for better control (such as *view only*).

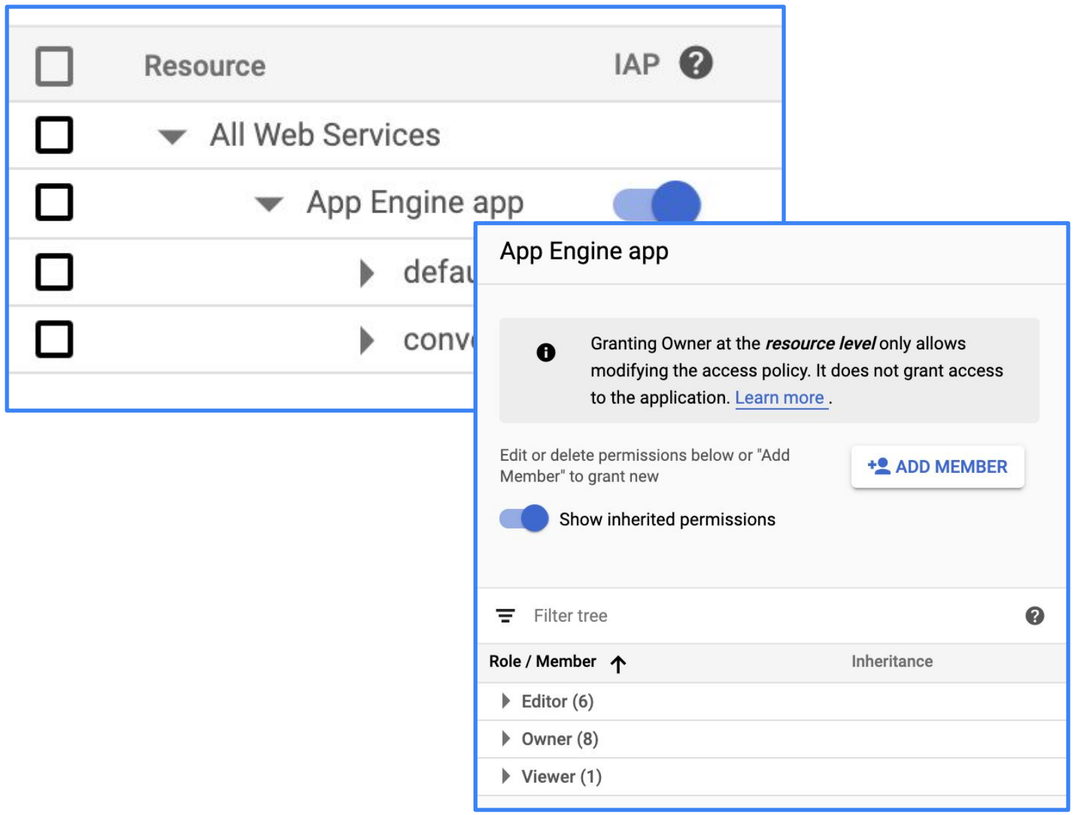
Roles

- Prefer pre-defined roles over custom roles.
- Grant roles at the smallest scope needed (least privilege).
- Limit use of “owner” and "editor" roles.
- Consider hierarchy inheritance when assigning roles.



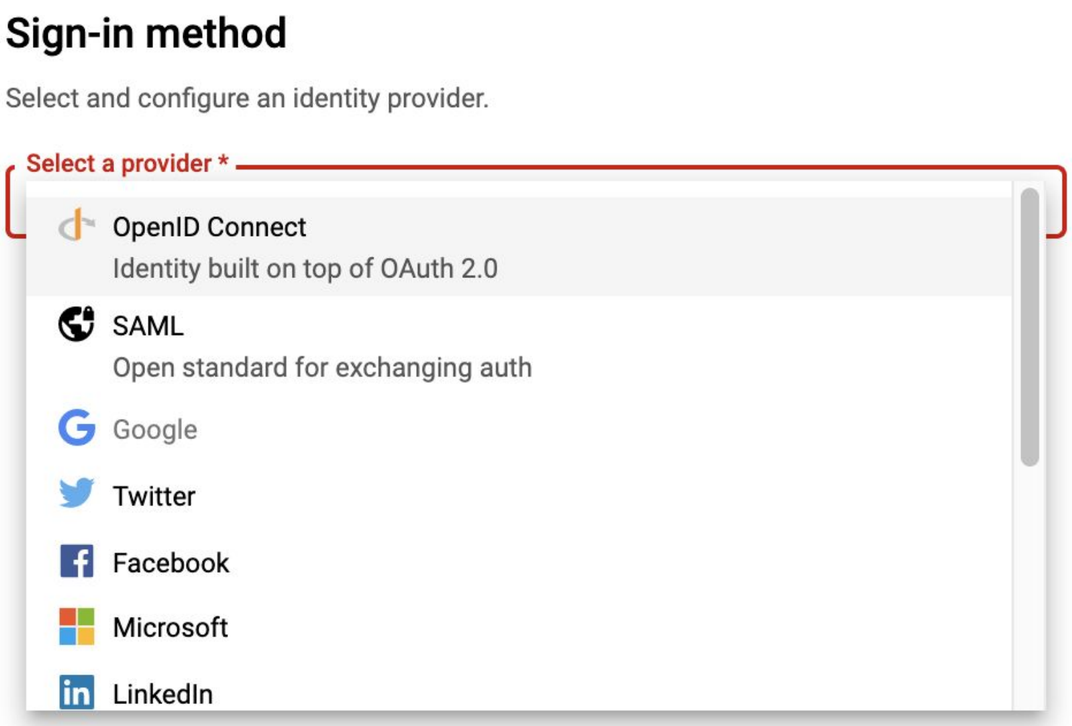
Identity-Aware Proxy simplifies authorization to Google Cloud applications and VMs

- Works with applications deployed behind the HTTP(S) load balancer in Compute Engine, GKE, or App Engine.
- When configured, it forces users to log in.
- Admins control who can access to app.
- Allows employees to securely access web-based applications without the need for a VPN.



Identity Platform provides authentication as a service

- Provides federated login that integrates with many common providers.
- Use it to provide sign-up and sign-in for your end users' applications.



Agenda

Security Concepts

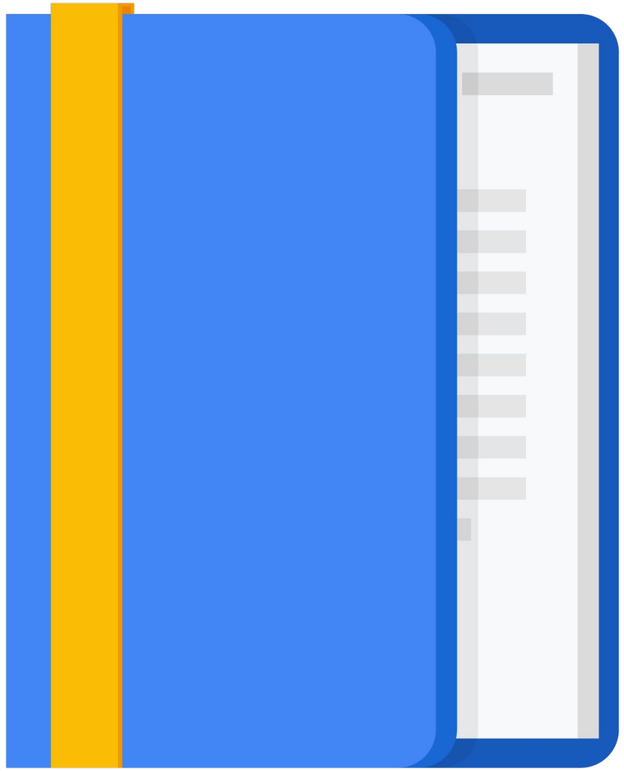
Securing People

Securing Machine Access

Network Security

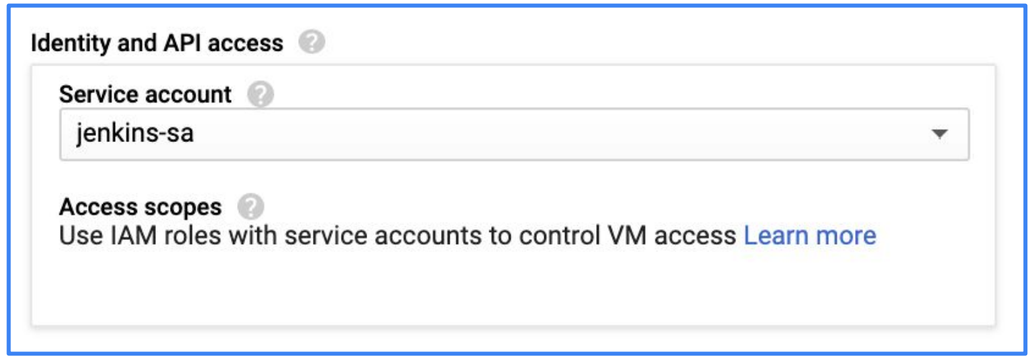
Encryption

Design Activity #12



Service accounts can be used for machine or application identities

- Create a service account and grant it one or more roles.
- Can assign that service account to VMs or GKE node pools.
- Those machines run with only the rights granted by the roles.



- Generate and download a key when creating a service account.
- This key can used for authentication.
- Key is downloaded as JSON.
- Store the key safely.

Can use service account keys to configure the CLI

- Allows you to grant controlled Google Cloud access to developers without giving them access to the Cloud Console.
- Also useful for automation when configuring VMs to run CI/CD pipelines.
- Use: `gcloud auth activate-service-account --key-file=[PATH TO KEY FILE]`

Agenda

Security Concepts

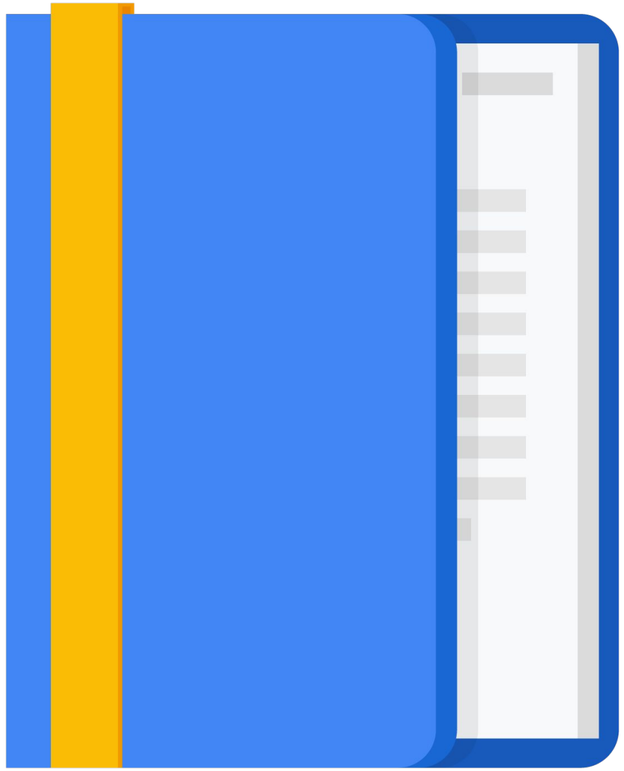
Securing People

Securing Machine Access

Network Security

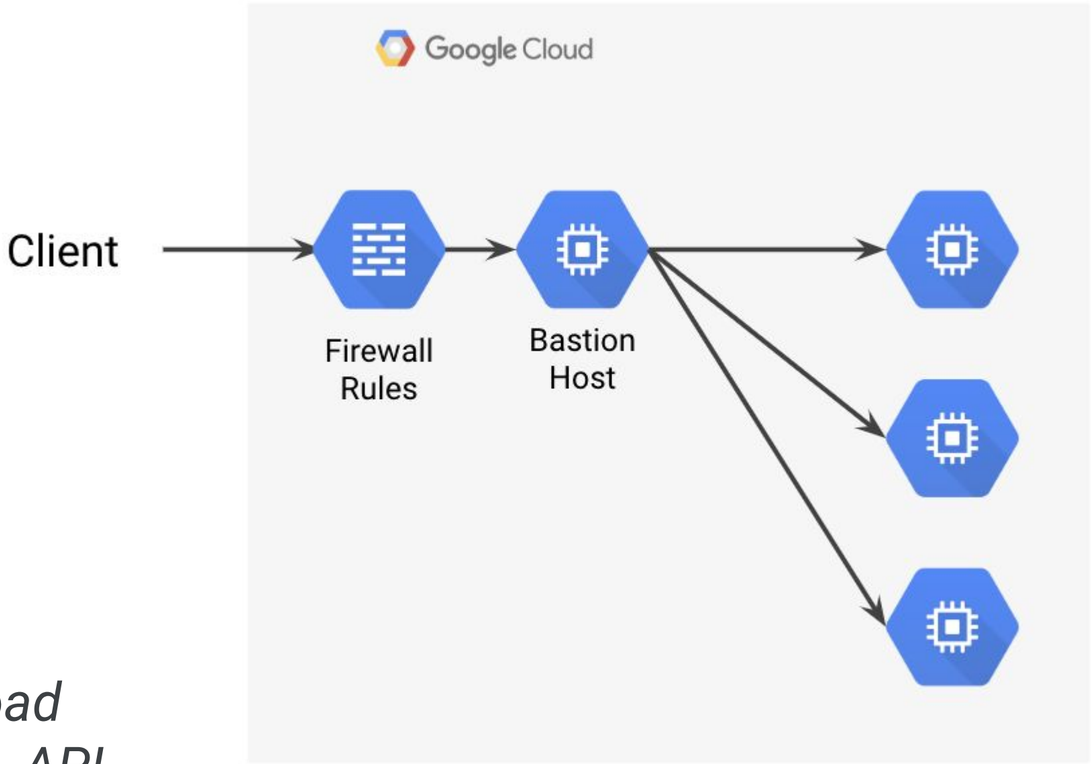
Encryption

Design Activity #12



Remove external IPs to prevent access to machines outside their network

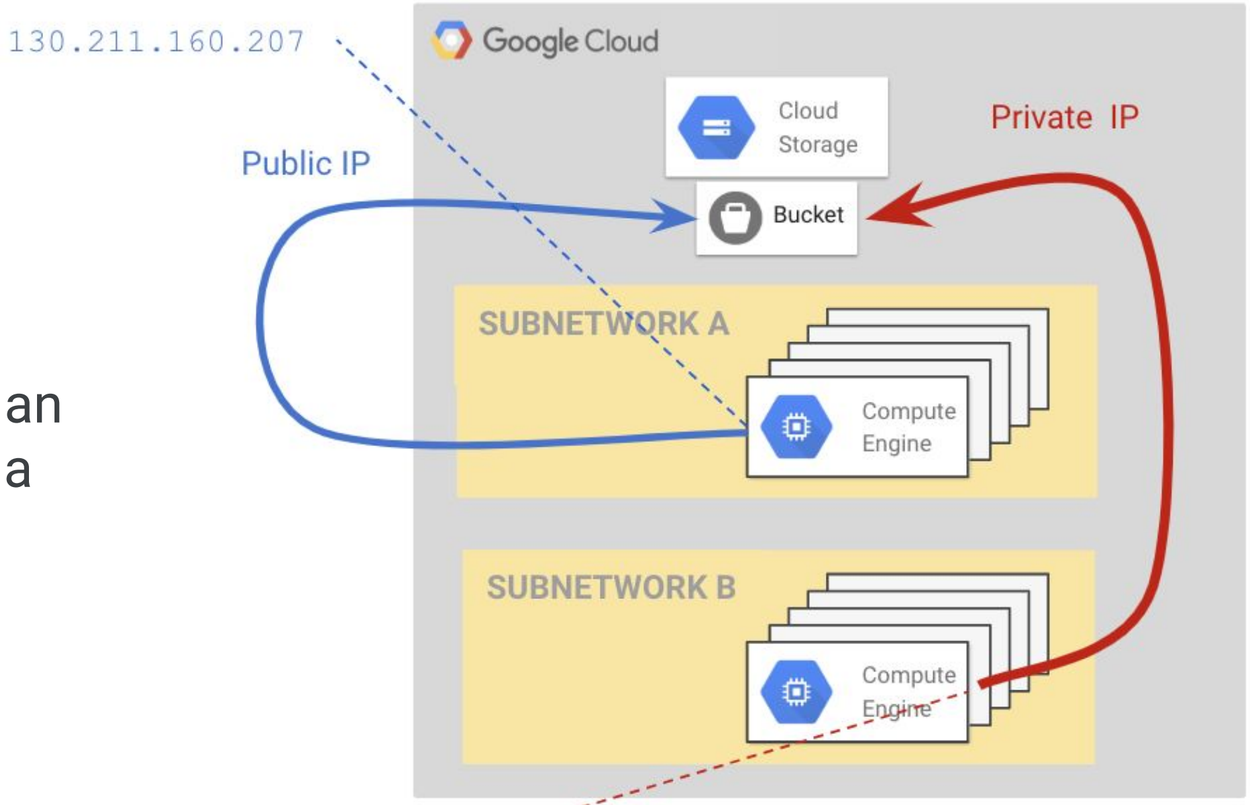
- Use a bastion host to provide access to private machines.
- Can also SSH into internal machines using Identity-Aware Proxy from the console and CLI.
- Use Cloud NAT to provide egress to the internet from internal machines.



All internet traffic should terminate at a load balancer, third-party firewall (proxy or WAF), API Gateway, or IAP. That way, internal services cannot be launched and get public IP addresses.

Private access allows access to Google Cloud services using an internal address

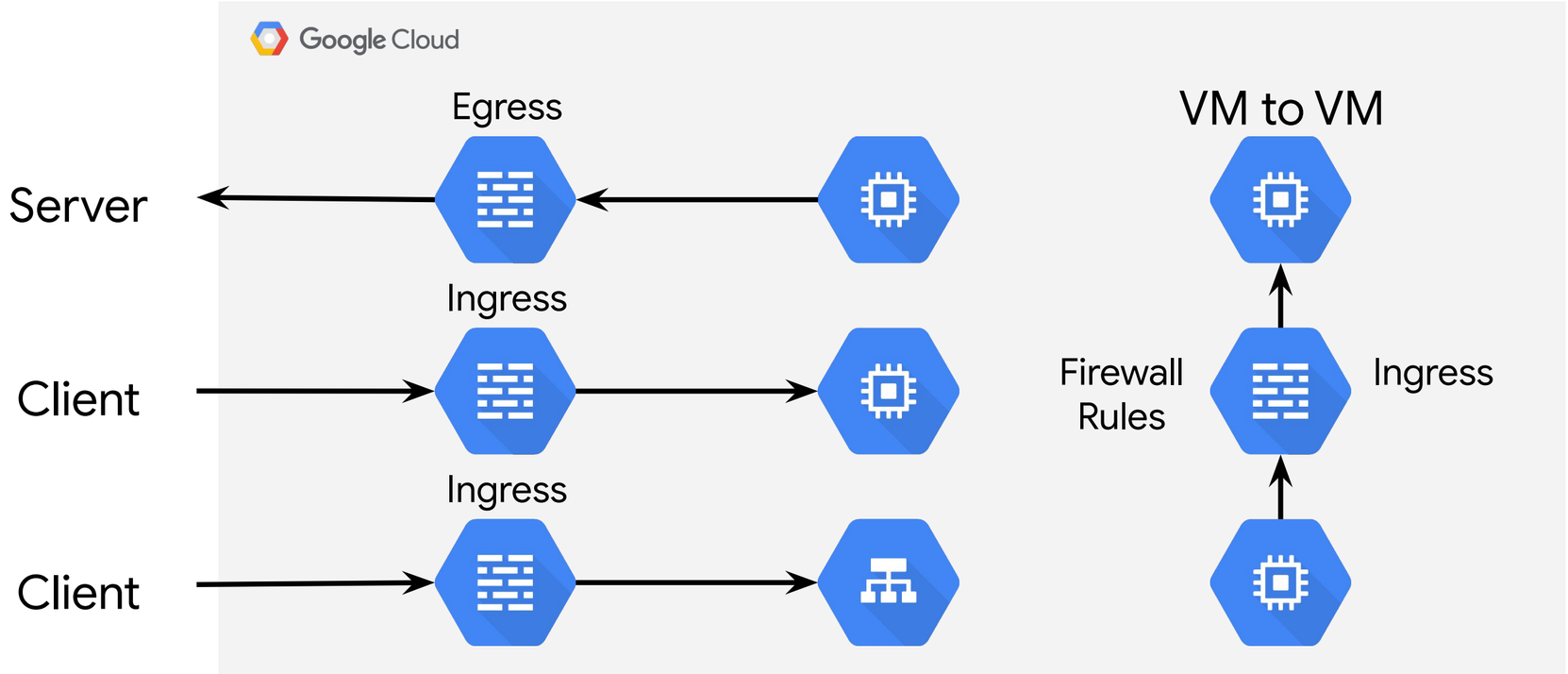
- Enabled when creating subnets.
- Allows access to Google Cloud services from VMs that only have internal IPs.
  - For example, a machine with only an internal IP would be able to reach a Cloud Storage bucket.




```
gcloud compute networks subnets
update subnet-b \
    --enable-private-ip-google-access
```

Configure firewall rules to allow access to VMs

- By default, ingress on all ports is denied.
- Add firewall rules to control which clients have access to which VMs on which ports.
- Application level security is the responsibility of the customer.

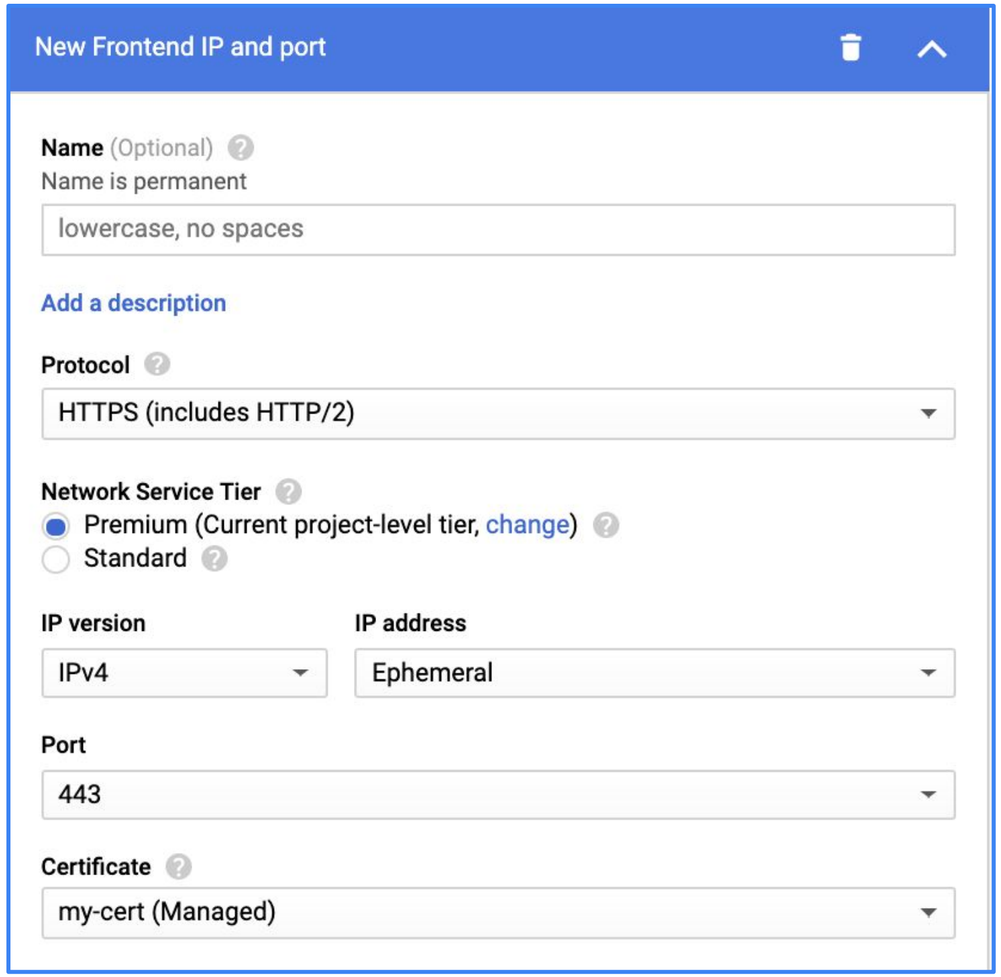


Control access to APIs using Cloud Endpoints

- Protect and monitor your public APIs.
- Control who has access to your API.
- Validate every call with JSON Web Tokens and Google API keys.
- Integrates with Identity Platform.

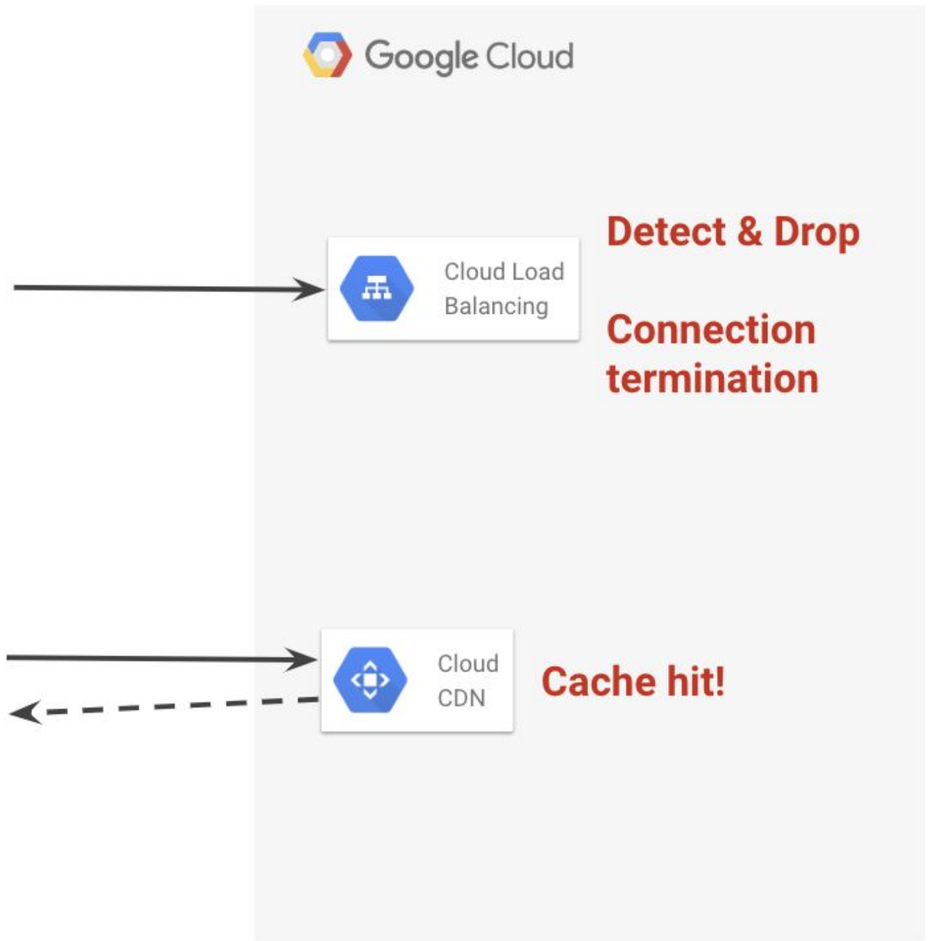
Restrict access to your services to TLS only

- All Google Cloud service endpoints use HTTPS.
- It's up to you to configure your service endpoints.
- In the load balancer setup, only create a secure frontend.



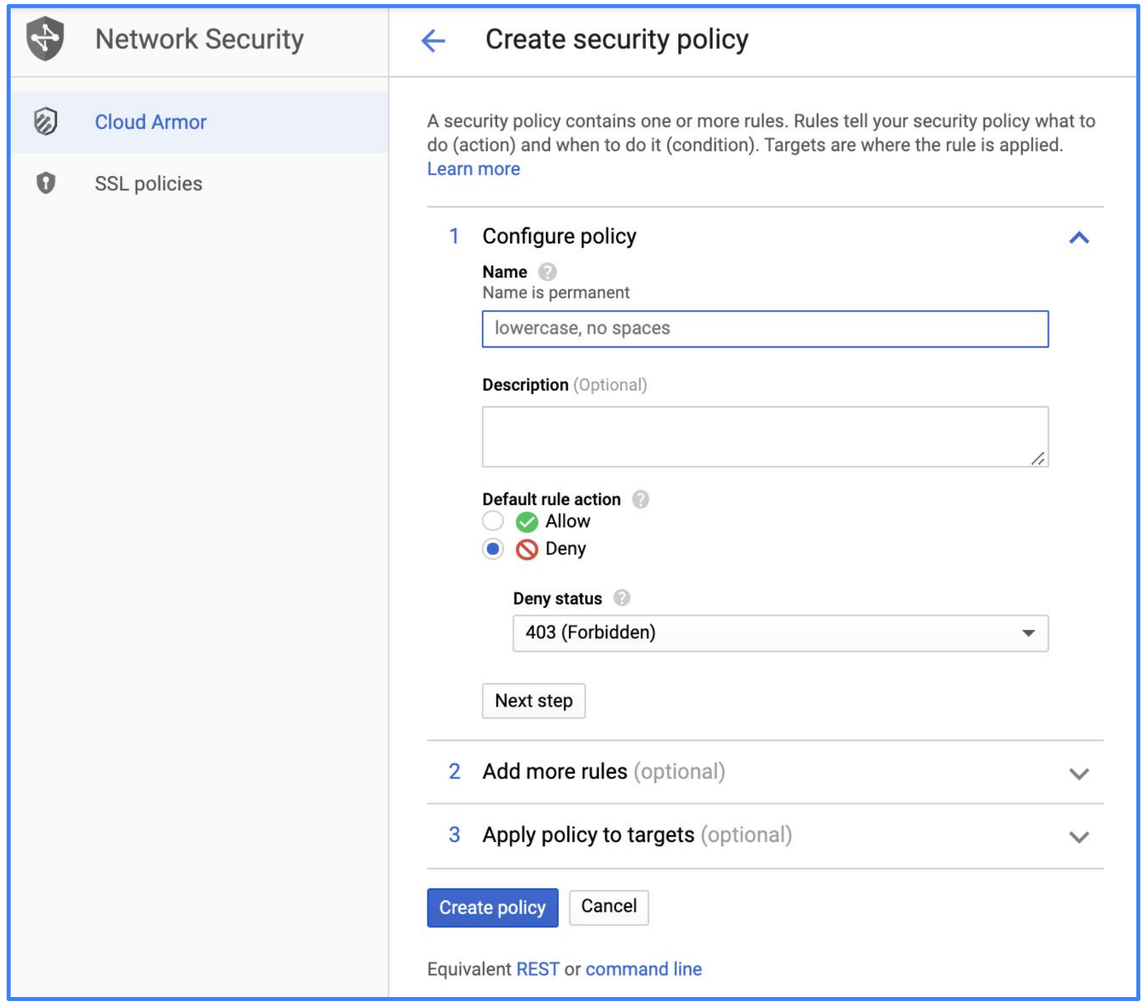
Leverage Google Cloud network services for DDoS protection

- Global load balancers detect attacks and drop them.
- Enabling the CDN will protect backend resources.



Use Cloud Armor to create network security policies

- Can allow or deny access to your Google Cloud resources using IP addresses or ranges.
- Create whitelists to allow known addresses.
- Create blacklists to block known attackers.



Cloud Armor supports layer 7 web application firewall (WAF) rules

- Predefined rules for preventing common attacks like SQL injection and cross-site scripting
- Flexible rules language allows you to allow or deny traffic using request headers, geographic location, ip addresses, cookies, etc.
- Examples:

```
inIpRange(origin.ip, '9.9.9.0/24')
request.headers['cookie'].contains('80=BLAH')
origin.region_code == 'AU'
inIpRange(origin.ip, '1.2.3.4/32') &&
request.headers['user-agent'].contains('WordPress')
evaluatePreconfiguredExpr('xss-canary')
```

Agenda

Security Concepts

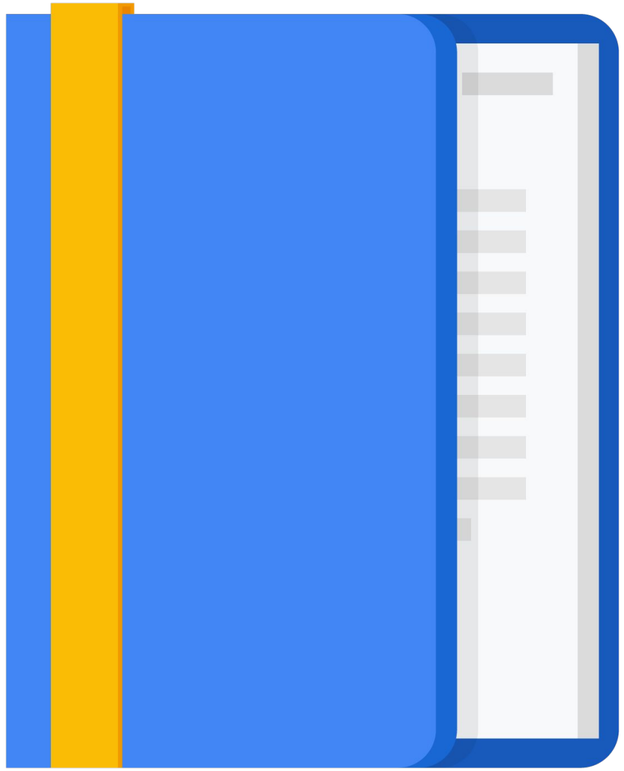
Securing People

Securing Machine Access

Network Security

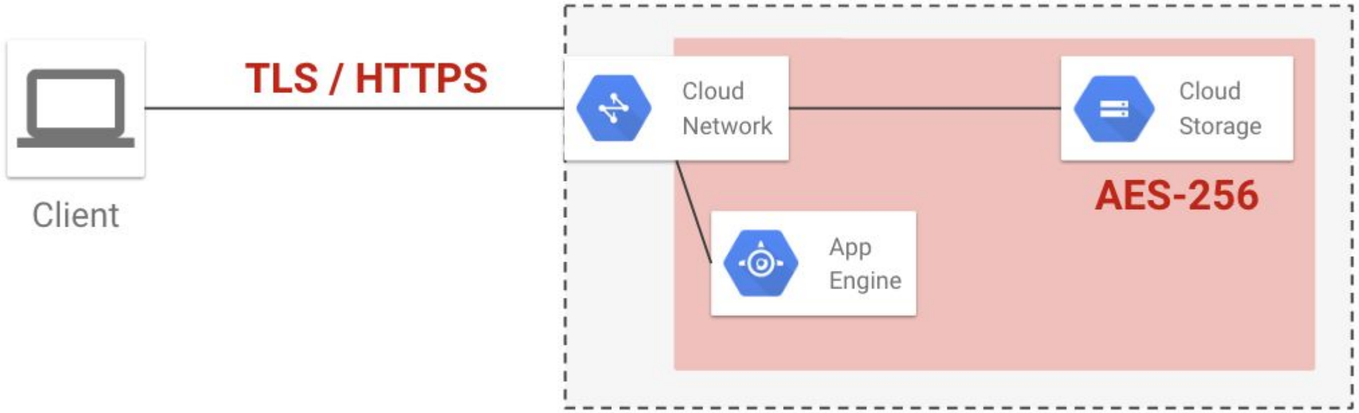
Encryption

Design Activity #12



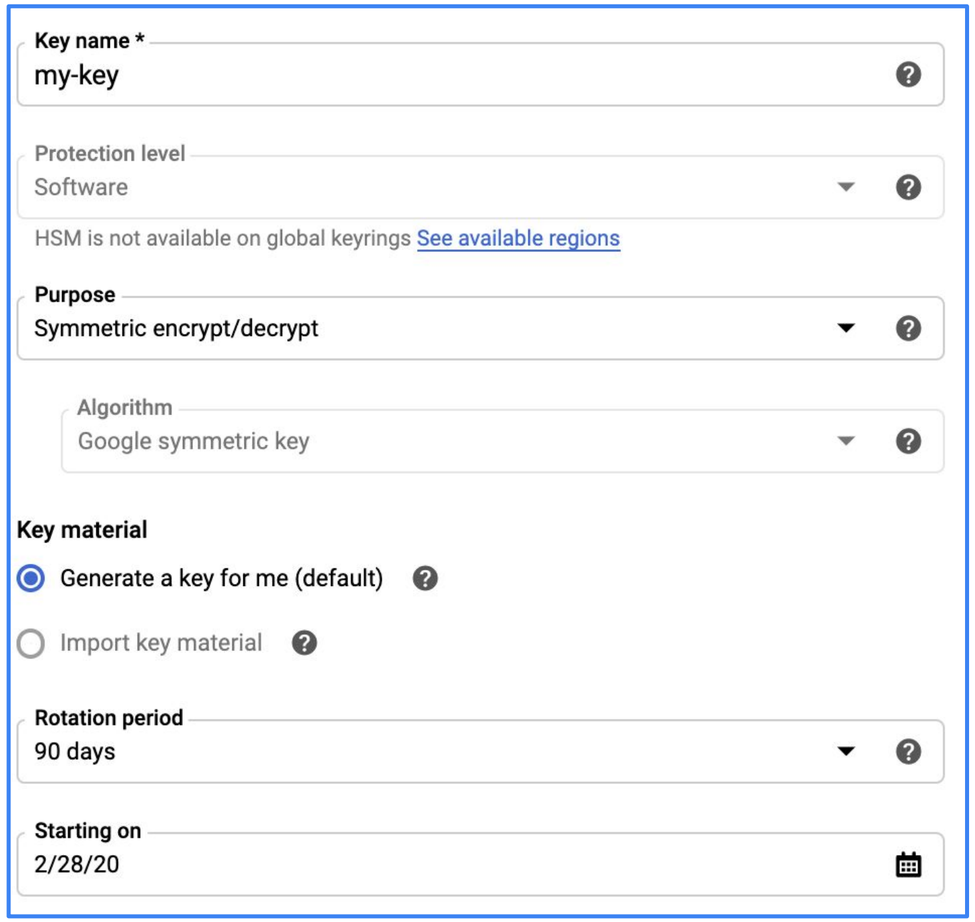
Google Cloud provides server-side encryption of data at rest by default

- Data Encryption Key (DEK) uses AES-256 symmetric key.
- Keys are encrypted by Key Encryption Keys (KEK).
- Google controls master keys in Cloud KMS.
- Keys are automatically periodically rotated.
- On-the-fly decryption by authorized user access with no visible performance impact



For compliance reasons, you may need to manage your own keys

- Customer-managed encryption keys are created in the cloud using Cloud Key Management Service (KMS).
- You create the keys and specify the rotation frequency.
- You can then select your keys when creating storage resources like bucket and disks.



Customer-supplied encryption keys are created in your environment and provided to Google Cloud

- Use your own keys with Google Cloud services.
- CSEK are supplied by the calling application per-API call.
- Only cached in RAM by Google.
- They decrypt a single payload (or column) or block of returned data.
- Supported by Compute Engine (persistent disks) and Cloud Storage.

The Data Loss Prevention API can be used to protect sensitive data by finding it and redacting it

- Scans data in Cloud Storage, BigQuery, or Datastore.
- Can also scan images.
- Detects many different types of sensitive data, including:
  - Emails
  - Credit cards
  - Tax IDs
- You can add your own information types.
- Can delete, mask, tokenize, or just identify the location of the sensitive data.

Activity 12: Modeling Secure Google Cloud Services

Refer to your Design and Process Workbook.

- Draw a diagram that depicts your case study security requirements.

Quiz

What Google Cloud service can you use to enforce the principle of least privilege when using Google Cloud?

A. IAM members and roles

B. Firewall rules

C. Encryption keys

D. SSL certificates

Quiz

What Google Cloud service can you use to enforce the principle of least privilege when using Google Cloud?

A. IAM members and roles

B. Firewall rules

C. Encryption keys

D. SSL certificates

Quiz

You don’t want programmers to have access to production resources. What’s the easiest way to do this in Google Cloud?

A. Create a firewall rule that blocks developer access to production servers and databases.

B. Create development and production projects, and don’t give developers access to production.

C. Use different service accounts for production and development resources with your project.

D. Set up private access and Identity-Aware Proxy.

Quiz

You don't want programmers to have access to production resources. What's the easiest way to do this in Google Cloud?

A. Create a firewall rule that blocks developer access to production servers and databases.

B. Create development and production projects, and don't give developers access to production.

C. Use different service accounts for production and development resources with your project.

D. Set up private access and Identity-Aware Proxy.

Quiz

Which Google Cloud features could help prevent DDoS attacks?

A. HTTP global load balancer

B. CDN

C. Google Cloud Armor

D. All of the above

Quiz

Which Google Cloud features could help prevent DDoS attacks?

A. HTTP global load balancer

B. CDN

C. Google Cloud Armor

D. All of the above

Quiz

What do you have to do to enable encryption when using Cloud Storage?

A. Simply enable encryption when configuring a bucket.

B. Enable encryption and upload a key.

C. Create an encryption key using Cloud Key Management Service, and select it when creating a Cloud Storage bucket.

D. Nothing: encryption is enabled by default.

Quiz

What do you have to do to enable encryption when using Cloud Storage?

A. Simply enable encryption when configuring a bucket.

B. Enable encryption and upload a key.

C. Create an encryption key using Cloud Key Management Service, and select it when creating a Cloud Storage bucket.

D. Nothing: encryption is enabled by default.

Review

Security

More resources

Google Cloud security products
https://cloud.google.com/security/products/

Encryption at rest
https://cloud.google.com/security/encryption-at-rest/default-encryption/

Encryption in transit
https://cloud.google.com/security/encryption-in-transit/

Google Cloud