Google Cloud Platform (GCP) Infrastructure Security

Prepared by: Adam Josevski and
Warrick Bickerton

Contents

This project will focus on the security aspect of infrastructure being deployed for the web application. Cyber Security teams focus should be the following things:

- *To deploy the infrastructure, an (IAM) role is needed. The goal should be to narrow down the access policies to only give operating access on resources that are part of the infrastructure. This will prevent people from spinning up unwanted resources.*
- *Research about firewalls: This is an extensive task. Compare all types of firewalls available in GCP and create a document on pros and cons of each. After which a decision can be made on which firewall to choose by the team leaders.*
- *Password storage/Encryption: While deploying the infrastructure, we will create resources like a Database. These resources have their username and password which must be supplied when creating them. These can't be open to all in the code and hence need a secure way of storage. Find a way to store these credentials (You can take AWS Security Access Manager (SAM) as a reference point and find something similar in GCP). If secure storage doesn't work, discuss with DevOps on how we can encrypt it and keep it in a place where it can be accessed and decrypted when deployment of infrastructure is being done through automated scripts.*

IAM Roles:

Identity and Access Management (IAM) is a new version Role-Based Access Control (RBAC). Google cloud provides a IAM system which is utilised to only grant user access to google cloud services. This is also used to control unauthorised access to other resources within the google cloud to increase security measures and protect assets. IAM system uses the principle of least privilege when users are utilising the resources [1], which refers to the action of limiting users' permissions and access to resources within the scope of their immediate tasks or responsibilities [2].

IAM in google cloud is extremely useful to implement within redback operations for several reasons. It allows the admins of Redback operations to authorise the users access and control on certain resources in a central manner. IAM in google cloud has great tools that are utilised to organise resource permissions with automation to help admins. IAM helps the admins to define default permissions for groups and only allow users access to resources to complete their job. Google Cloud has a service called Recommender which is a machine learning tool that is used to remove unwanted access from resources. Recommender automatically detects permissions and access that are authorised more than what is needed and reduces the access based on similar roles [2].

IAM has features that enables admins to create access control policies on resources based on conditions such as IP address, security status of the device, type of resource and date. Administrators will also be able to see a full audit history including permissions authorisation, removal of permissions autonomously. They also will have the ability to create user accounts based on applications and resources. From the Google Admin Console, they can manage users and group, implement security methods such as single sign-on and set up two-factor authentication [2]. A great introduction video can be shown here [3] Cloud IAM in a minute

https://cloud.google.com/iam/docs/overview

How IAM Works:

IAM allows you to manage access control by defining the identity and access (role) to certain resources. Resources include the organisations, folders, and projects that you use to arrange your resources. Permission to use a resource is not given directly to the user under IAM. Instead, permissions are organised into roles, which are assigned to authenticated principals. An allow policy within an IAM, establishes and maintains which principals are assigned to the roles. Each policy belongs to a resource. When an authenticated principal tries to access a resource, IAM verifies the allow policy of a resource to ensure that the activity is allowed [4].

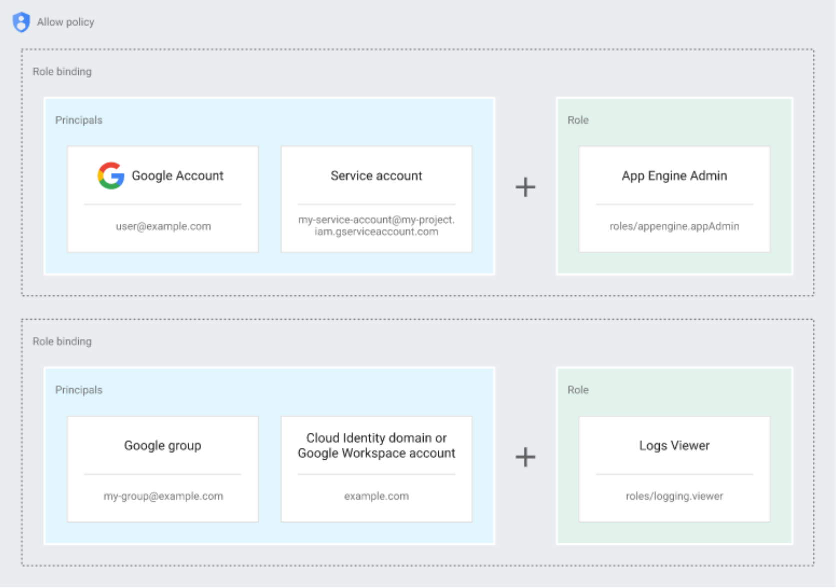

Figure 1 from [4]

Access management has three parts, and they include principals, role and allow policy. Principals involve a Google Account (users), a service account (apps/computing workloads), a group, a Google Workspace account, or a Cloud Identity domain. Each principle is uniquely identified. A role is basically a set of permissions. Permissions control what actions are permitted on a particular resource. The allow policy is a set of role bindings that assign one or more principals to the specific role. A allow policy you must link it to a resource to define the principal and role (access) [4].

The types of roles for IAM

- Basic Role: Includes owner, editor and viewer (not recommended)
- Predefined Role: Google creates and maintains predefined roles that offer more access to the specified Google Cloud resources while not allowing unauthorised access to other resources.
- Custom Role: Roles that you can create and you can establish custom roles to adjust permissions to your needs.
- The actions that can be performed on resources: Create, modify, delete

Reference [4]

Sample Allow Policy:

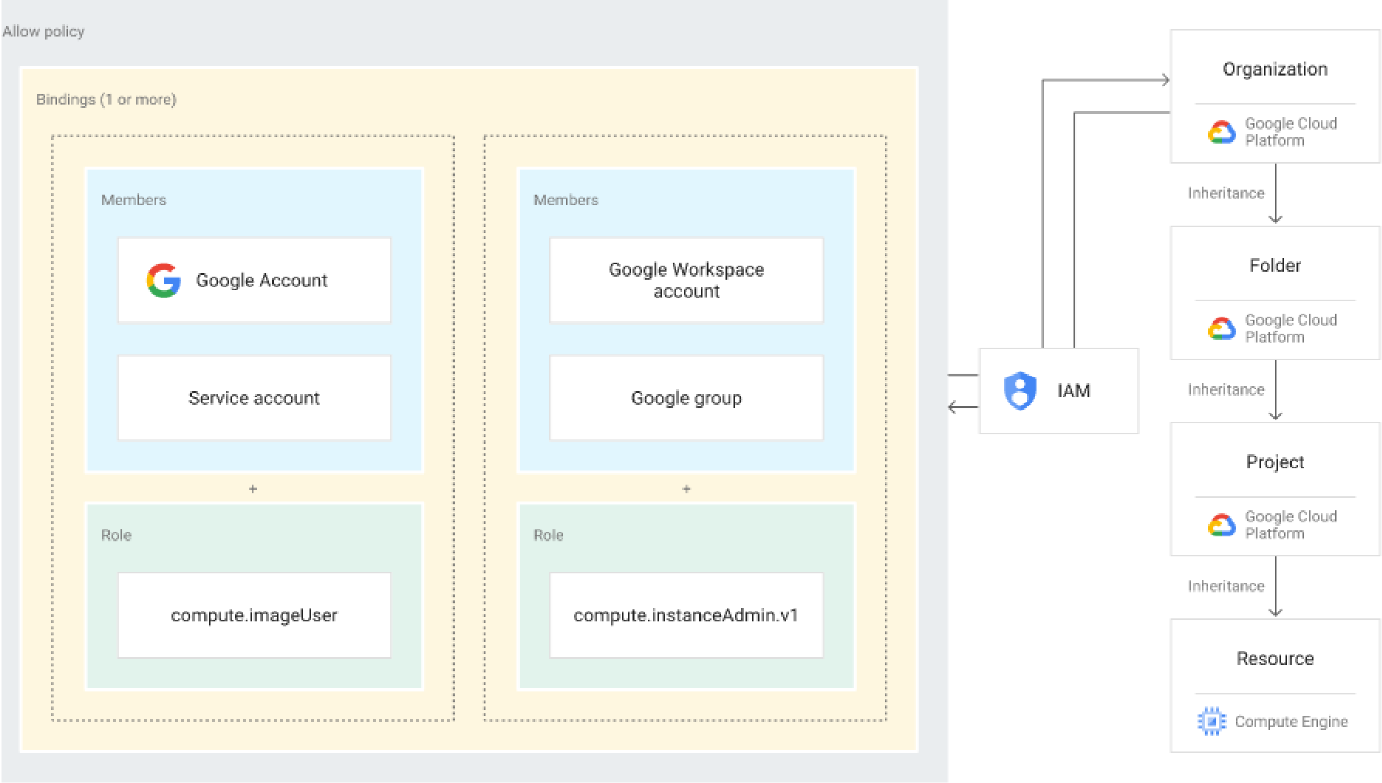

Figure 2 from [4]

IAM Recommendations

Redback operations should implement the following for IAM:

- Custom roles for each resource
- Create IAM policies based on least privilege
- Create a user with their assigned role
- Add resources/actions in a IAM policy
- Attach the policy to the user
- Read and follow reference [5]

Firewalls within Google Cloud

Google Cloud allows hierarchical firewall policies. This lets Redback implement a firewall policy (collection of firewall rules) across the entire google cloud platform (GCP) organization. The hierarchy of the GCP is shown below in figure 3, therefore making it easier to implement and enforce consistent firewalls across the Redback’s GCP environment [7].

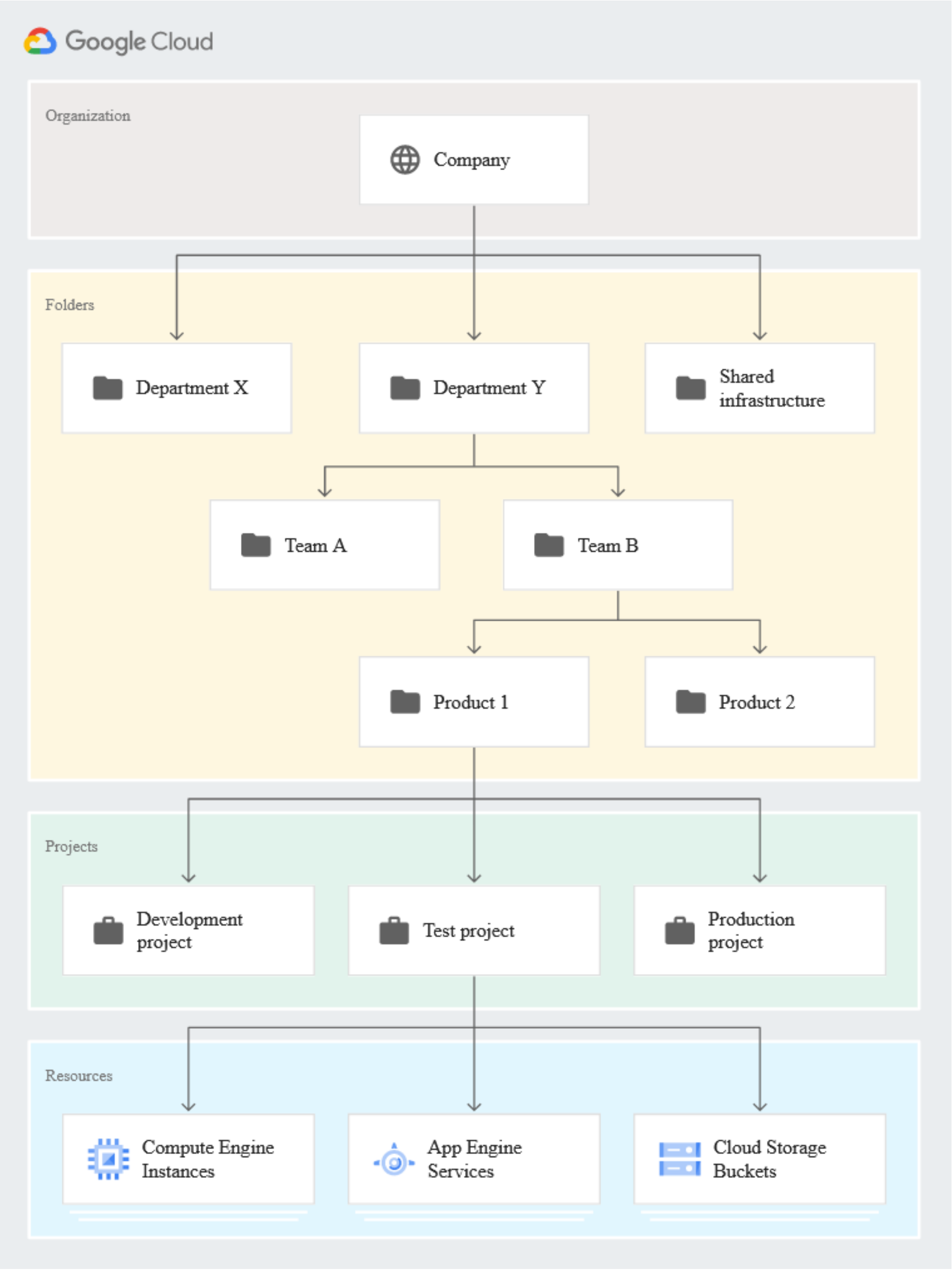

Figure 3 from [24]

Firewall policies can be implemented at the organizational, folder, and resources (Virtual private cloud) level as VPC firewalls are applied to a GCP project [12]. Hierarchy firewall policies are evaluated in hierarchical order, meaning that lower-level rules cannot override a rule implemented from a higher level.

For example, Redback's organizational firewall policy will be evaluated first, then the folder firewall policy, and lastly the VPC rules [8]. If a firewall rule with a policy is found to be a match, then the policy action is taken (permit or deny) and all other lower-level policy rules in the hierarchy are ignored unless "go to next" is the rule action.

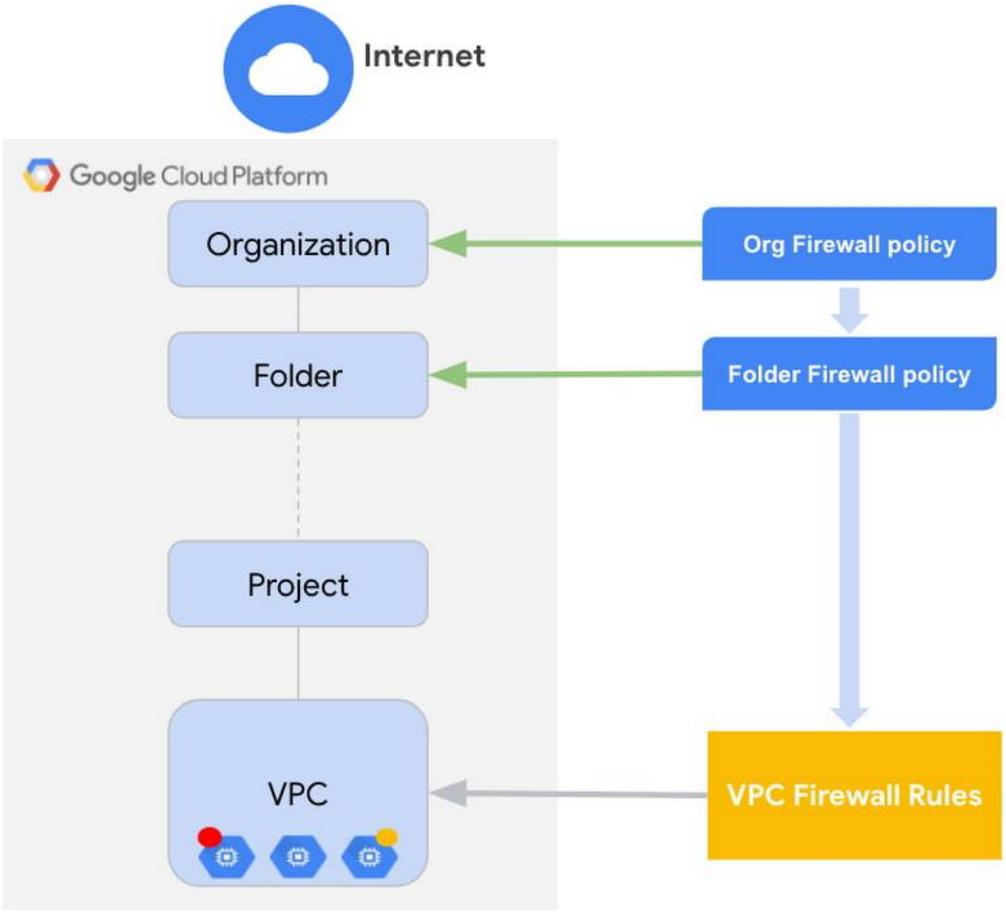

Figure 4 from [25]

All three types of Firewall implementations (Organisation, folder, and VPC) are enforced at the VM level and not applied at the edge of the network like a traditional firewall device [9]. Instead, each VPC firewall functions as a distributed firewall [10] (host-resident security software application [11]). Therefore, the VPC firewall rules exist between instances and other networks, but also between induvial instances on the same network [12].

Organisational and folder firewall policies are defined in the GCP organization security policy resource which acts as a central container for the firewall rules [14] and is created at the organization and folder nodes [7].

If Redback chooses to implement VPC firewall rules it will allow us to permit or block connections to or from the virtual machine/s and are the most granular type of firewall within GCP [12]. Enabled VPC firewall rules are always in operation providing protection to an instance regardless of configuration, operation system, and whether the instance has started up or not [12]. All VPC firewall rules are stateful rather than stateless, meaning the firewall constantly monitors and tracks the state of active connections while at the same time examining incoming traffic to discover potential traffic and data risks [13].

Pros and Cons of each type of firewall in GCP

Firewall Type	Pros	Cons
Organizational Firewall policy	• Proves a simple, consistent, and reliable way to enforce firewall rules over Redback's entire organization (all projects and VPCs).	• Misconfigured firewalls can bring down Redback's entire cloud platform and allow unauthorized traffic to certain VMs.
Folder Firewall policy	• Targets mid-level nodes (folders) where VPCs can inherit networks and firewall policies. Good for policies that apply to all VPCs of a node but not the entire organization.	• Not granular enough to apply different VPC rules to specific VMs if they require different Firewall rules.
VPC Firewall Rules	• Very granular and can be individually tailored to meet any specific VMs firewall requirements.	• If all firewalls are implemented at the VPC level, there may be duplications which can cause unnecessary resource usage and confusion for Redbacks Cloud administrators.

All three different types of Firewall policies and rules should be implemented together as they serve different purposes. Below Figure 5 is an example of this.

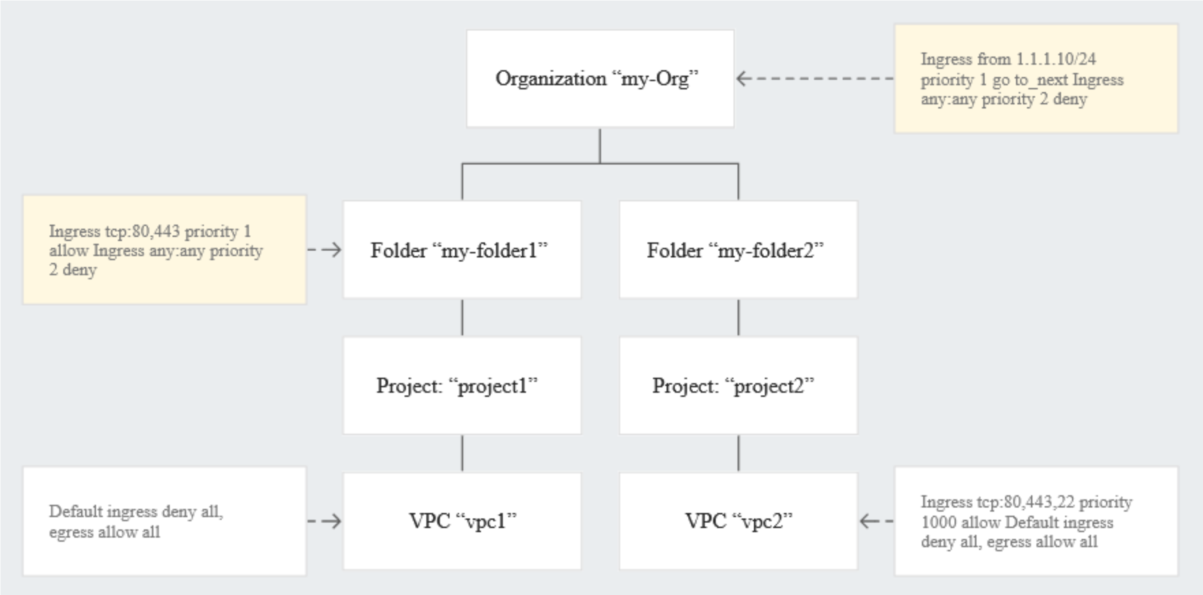
Organization “my-Org”
Ingress from 1.1.1.10/24 priority 1 go to_next Ingress any:any priority 2 deny
Ingress tcp:80,443 priority 1 allow Ingress any:any priority 2 deny
Folder “my-folder1”
Folder “my-folder2”
Project: “project1”
Project: “project2”
Default ingress deny all, egress allow all
VPC “vpc1”
VPC “vpc2”
Ingress tcp:80,443,22 priority 1000 allow Default ingress deny all, egress allow all

Figure 5 from [26]

Firewall Recommendations

When implementing firewall rules within GCP Redback should consider the following best practices recommended by Google Cloud:

- Principle of least privilege is implemented. Therefore, all traffic is blocked by default, and only specific traffic that is needed is allowed [12].
- Hierarchical firewall policy rules are used to deny traffic that is not permitted at an organization or folder level [12].
- Permit or “Allow” rules in GCP should be restricted to specific VMs by specifying the VMs unique service account [12].
- If firewall rules are created based on IP Addresses (IPV4 and IPV6), try to keep the number of rules to a minimum [12]. As it is easier to track a single rule that allows traffic to 10 VMs than it is to track 10 separate rules between separate VMs.
- GCP’s Firewall Rules logging function should be turned on and the Firewall Insights function is used to confirm that the firewall rules are functioning as intended [12]. GCP’s Firewall Rules logging function does incur extra costs [12].

Google Cloud Secret Manager

The secret manager from google cloud provides Redback with the ability to natively store passwords, API keys, and certificates on Google Cloud [15]. These secrets are stored and accessed as binary blobs or text strings [16]. Authorized users can then be assigned the appropriate permissions to view the contents of the secrets [16], enforcing the principle of least privilege.

Secrets

In relation to Google's Secret Manager, a 'Secret' is a globally accessible object that exists at the project level within the GCP structure [16]. This 'Secret' object contains a collection of metadata and secret versions [16].

Metadata can include:

- Replication locations [16]
- Labels [16]
- Annotations [16]
- Permissions [16]

Versions

Secret versions contain the actual secret data. i.e., credential or API key [16]. These versions can be addressed individually but cannot be modified only deleted [16]. Therefore, to modify a secret version you must create a new one.

Rotations

Secrets can be rotated by adding a new secret version to the secret [15]. All different versions of a given secret are accessible, provide that a specific version is enabled [15].

Google states [20] that recurring rotation of secrets helps:

- Minimize damage if a secret is leaked.
- Enforces correct access policy by denying access to previous secret holders who no longer need access to the secret as the old secret value has been rotated.

Furthermore, by disabling a specific version Redback can prevent that secret version from being used [15].

Encryption of secrets

By default, Google Cloud's Secret Manager always encrypts secret data before it is persisted to disk (Google clouds high-performance SSD and HDD block storage [18]) [17]. The API used for the Secret manager always sends traffic over a secure HTTPS connection [17]. Therefore, data is encrypted with TLS while in transit and with AES-256-bit encryption keys while at rest [15]. The major benefit of encrypting all data by default is that Redback does not have a setup or configure the encryption manually as it is already done [17].

Furthermore, Google states [17] that there is no visible degradation in performance when using its encryption service, and Redback's secret data will be automatically decrypted when accessed by a user who has the appropriate permissions [17], providing seamless access to users and administrators.

Database Passwords

Google states [16] that its secret manager works well for storing configuration information such as database passwords, which can be a major security risk to Redback's cloud infrastructure if not done correctly. Below is a brief video [19] explaining how Google's Cloud Code and Secret Manager can work together to achieve this.

Implementation Recommendations

Passing application secrets through Redback's codebase or filesystem is common in deployment environments [21]. Google recommends that this should be avoided when possible because:

- If Redback's secret is readily accessible on the filesystem, it increases the severity and impact of application vulnerabilities. For example, a vulnerability such as a directory traversal attack will enable a hacker to gain a way to view secret data as the secret is accessible [21].
- Consuming secrets through environment variables increase the risk of misconfigurations that leak secrets. For example, a log process environment detail that leaks secrets [21].

Because of the reason mentioned above Google Cloud [21] recommends that if possible Redback should enable the Secret Manager API directly by using one the provided client libraries, which can be found at the following URL [22] https://cloud.google.com/secret-manager/docs/reference/libraries.

Glossary

Firewall – Either hardware device or software that monitors network traffic (incoming and outgoing) and determines whether to allow or block certain traffic (data packets) based on a defined set of security rules [6].

Principle of Least Privilege (PoLP) - CyberArk states [23] that PoLP Is a cybersecurity concept where users are granted minimum levels of access or permissions that is required to carry out their role/job functions.

References

[1] Google Cloud (n.d). *Access control for organizations with IAM* [Website]. Available: https://cloud.google.com/resource-manager/docs/access-control-org

[2] Google Cloud (n.d). *Identity and Access Management (IAM)* [Website]. Available: https://cloud.google.com/iam

[3] Google Cloud Tech (2021, July 19). "Cloud IAM in a minute" *YouTube*. [Video file]. Available:https://www.youtube.com/watchv=zd5d9Vv1ZFE&ab_channel=GoogleCloudTech

[4] Google Cloud (n.d). *IAM overview* [Website]. Available: https://cloud.google.com/iam/docs/overview

[5] Google Cloud (n.d). *How-to guides (IAM)* [Website]. Available: https://cloud.google.com/iam/docs/how-to

[6] Cisco (n.d). *What Is a Firewall?* [Website]. Available: https://www.cisco.com/c/en_au/products/security/firewalls/what-is-a-firewall.html

[7] Google Cloud (n.d). *Hierarchical firewall policies overview* [Website]. Available: https://cloud.google.com/vpc/docs/firewall-policies

[8] Google Cloud (2020, August 6). "How do I provide organizational wide security control using Hierarchical Firewall Policies" *YouTube*. [Video file]. Available: https://www.youtube.com/watch?v=Z_S7tHKxadU

[9] Google Cloud (2021, March 3). *Managing cloud firewalls at scale with new Hierarchical Firewall Policies* [Website]. Available: https://cloud.google.com/blog/products/identity-security/new-google-cloud-hierarchical-firewall-policies

[10] S. Wong (2019, April 30). *Protect your Google Cloud Instances with Firewall Rules* [Website]. Available: https://stephrwong.medium.com/protect-your-google-cloud-instances-with-firewall-rules-69cce960fba

[11] Barracuda (n.d). *Distributed Firewall* [Website]. Available: https://www.barracuda.com/glossary/distributed-firewall

[12] Google Cloud (n.d). *VPC firewall rules overview* [Website]. Available: https://cloud.google.com/vpc/docs/firewalls

[13] Fortinet (n.d). *Stateful Firewall* [Website]. Available: https://www.fortinet.com/resources/cyberglossary/stateful-firewall

[14] Google Cloud (2021. March 4). *Managing cloud firewalls at scale with new Hierarchical Firewall Policies* [Website]. Available: https://cloud.google.com/blog/products/identity-security/new-google-cloud-hierarchical-firewall-policies

[15] Google Cloud (n.d). *Secret Manager* [Website]. Available: https://cloud.google.com/secret-manager

[16] Google Cloud (n.d). *Secret Manager conceptual overview* Website]. Available: https://cloud.google.com/secret-manager/docs/overview

[17] Google Cloud (n.d). *Encryption of secrets* [Website]. Available: https://cloud.google.com/secret-manager/docs/encryption

[18] Google Cloud Tech (2020, August 17). "Persistent Disk in a minute" *YouTube*. [Video file]. Available: https://www.youtube.com/watch?v=zovhVfou-DI

[19] Google Cloud Tech (2021, February 23). "Cloud Code and Secret Manager integration" *YouTube*. [Video file]. Available: https://www.youtube.com/watch?v=uU-OnywmN_A&feature=emb_title

[20] Google Cloud (n.d). *Rotation of secrets* [Website]. Available: https://cloud.google.com/secret-manager/docs/rotation-recommendations

[21] Google Cloud (n.d). *Secret Manager Best Practices* [Website]. Available: https://cloud.google.com/secret-manager/docs/best-practices
[22] Google Cloud (n.d). *Secret Manager client libraries* [Website]. Available: https://cloud.google.com/secret-manager/docs/reference/libraries
[23] CYBERARK (n.d). *Principle of Least Privilege* [Website]. Available: https://www.cyberark.com/what-is/least-privilege/
[24] Google Cloud (n.d). *Resource hierarchy* [Website]. Available: https://cloud.google.com/resource-manager/docs/cloud-platform-resource-hierarchy
[25] Google Cloud (n.d). *Managing cloud firewalls at scale with new Hierarchical Firewall Policies* [Website]. Available: https://cloud.google.com/blog/products/identity-security/new-google-cloud-hierarchical-firewall-policies
[26] Google Cloud (n.d). *Hierarchical firewall policies overview [*Website]. Available: https://cloud.google.com/vpc/docs/firewall-policies