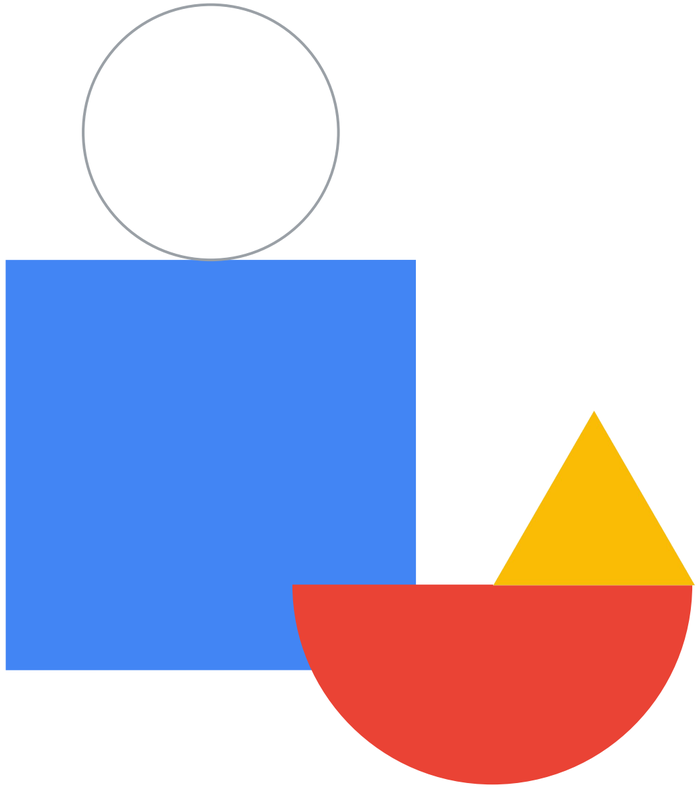
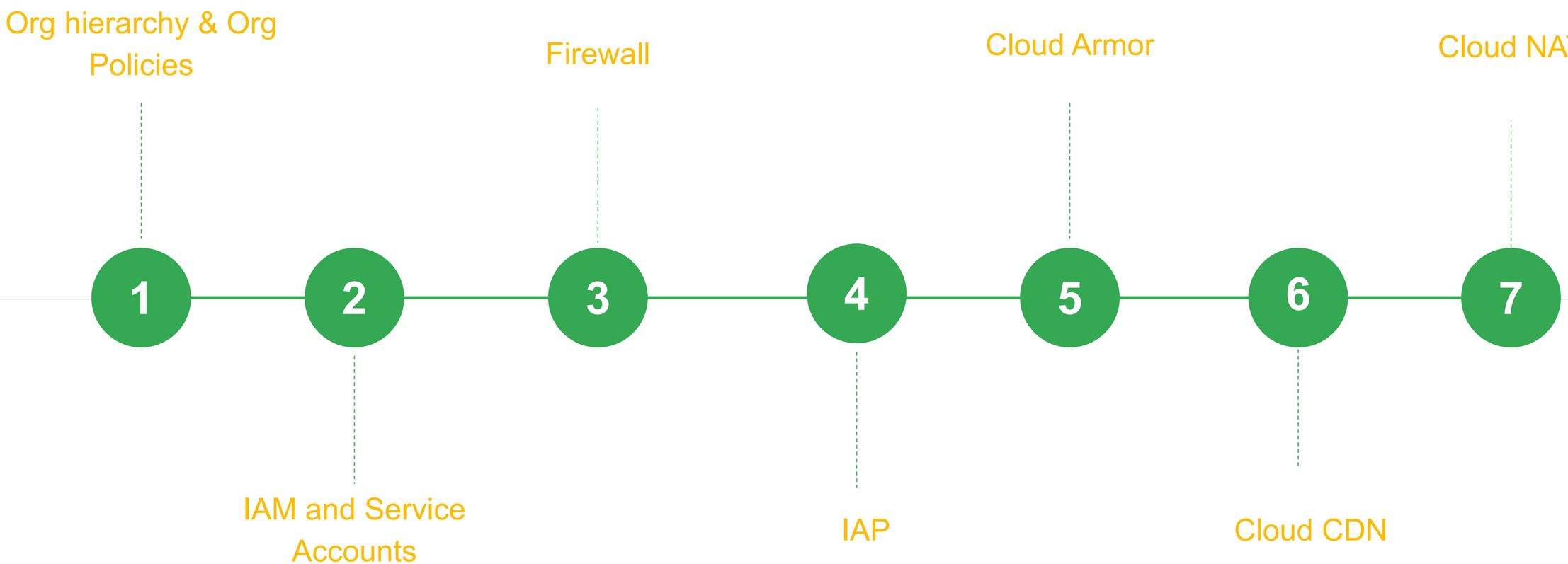
Google Cloud



Preparing for Your Professional Cloud Security Engineer Journey

Week 2 topics

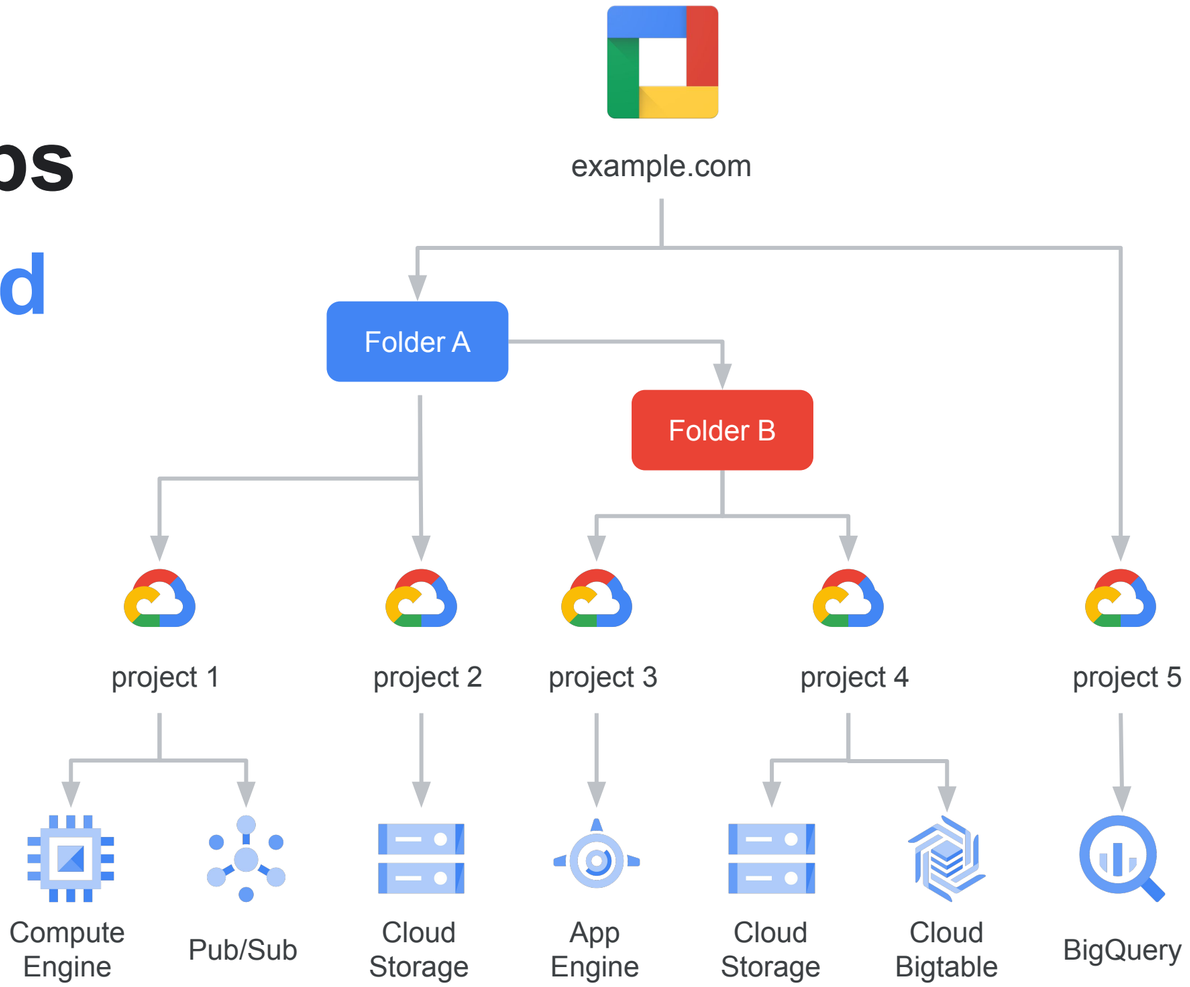


Organization Hierarchy And Org Policies

Organization hierarchy helps organize access control and policy for resources

Folders provide for flexible hierarchy of Projects

- Organization policy and access control can be bound at any level and flow downwards



[Know how to migrate projects across folders / orgs]

Organization policy pattern example

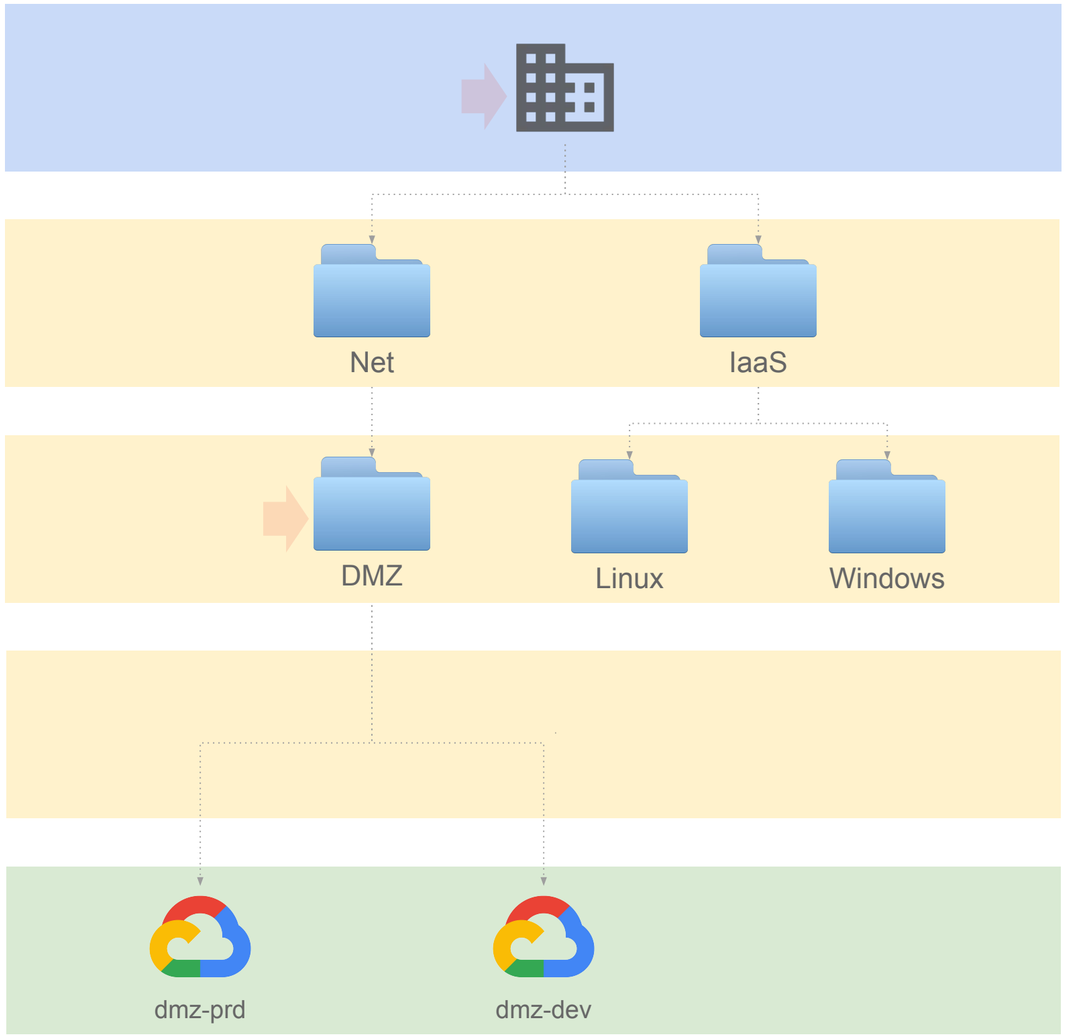
`constraints/compute.vmExternalIpAccess` → `false`

no VMs should be able to use external IPs

inheritance

`constraints/compute.vmExternalIpAccess` → `true`

DMZ appliances should be able to use external IPs



Most common Organization Policy constraints

Policy Constraint	Description
compute.vmExternalIpAccess	A list of project/zone/instance names that are allowed to have external IP addresses and deny all others. Attempts to create any other VMs with an external IP address will fail.
compute.trustedImageProjects	A list of projects that contain trusted images that can be used as the basis for a VM and deny all others. Attempting to instantiate a VM with an image from another project is denied.
compute.skipDefaultNetworkCreation	Disables the creation of default VPC when creating a project. The default VPC uses auto mode subnetworks and includes default firewall rules which are often incompatible with production deployments.
iam.disableServiceAccountKeyCreation	This boolean constraint disables the creation of service account external keys where this constraint is set to `True`.
compute.restrictVpcPeering	This list constraint defines the set of VPC networks that are allowed to be peered with the VPC networks belonging to this project, folder, or organization.
serviceuser.services	This list constraint defines the set of services and their APIs that can be enabled on this resource and below. By default, all services are allowed.
gcp.resourceLocations	BETA: This list constraint defines the set of locations where location-based GCP resources can be created. Policies for this constraint can specify multi-regions such as asia and europe, regions such as us-east1 or europe-west1, or individual zones such as europe-west1-b as allowed or denied locations.
sql.restrictPublicIp	This boolean constraint restricts configuring Public IP on Cloud SQL instances where this constraint is set to True. This constraint is not retroactive, Cloud SQL instances with existing Public IP access will still work even after this constraint is enforced. By default, Public IP access is allowed to Cloud SQL instances.
sql.disableDefaultEncryptionCreation	BETA: Restrict default Google-managed encryption on Cloud SQL instances
compute.requireShieldedVm	This boolean constraint, when set to True, requires that all new Compute Engine VM instances use Shielded disk images with Secure Boot, vTPM, and Integrity Monitoring options enabled. Secure Boot can be disabled after creation, if desired. Shielded VM features add verifiable integrity and exfiltration resistance to your VMs.
compute.restrictSharedVpcHostProjects	Restrict Shared VPC Host Projects This list constraint defines the set of Shared VPC host projects that projects at or below this resource can attach to. By default, a project can attach to any host project in the same organization, thereby becoming a service project.
iam.allowedPolicyMemberDomains	This list constraint defines the set of members that can be added to Cloud IAM policies. By default, all user identities are allowed to be added to Cloud IAM policies. The allowed/denied list must specify one or more Cloud Identity or G Suite customer IDs. If this constraint is active, only identities in the allowed list will be eligible to be added to Cloud IAM policies.

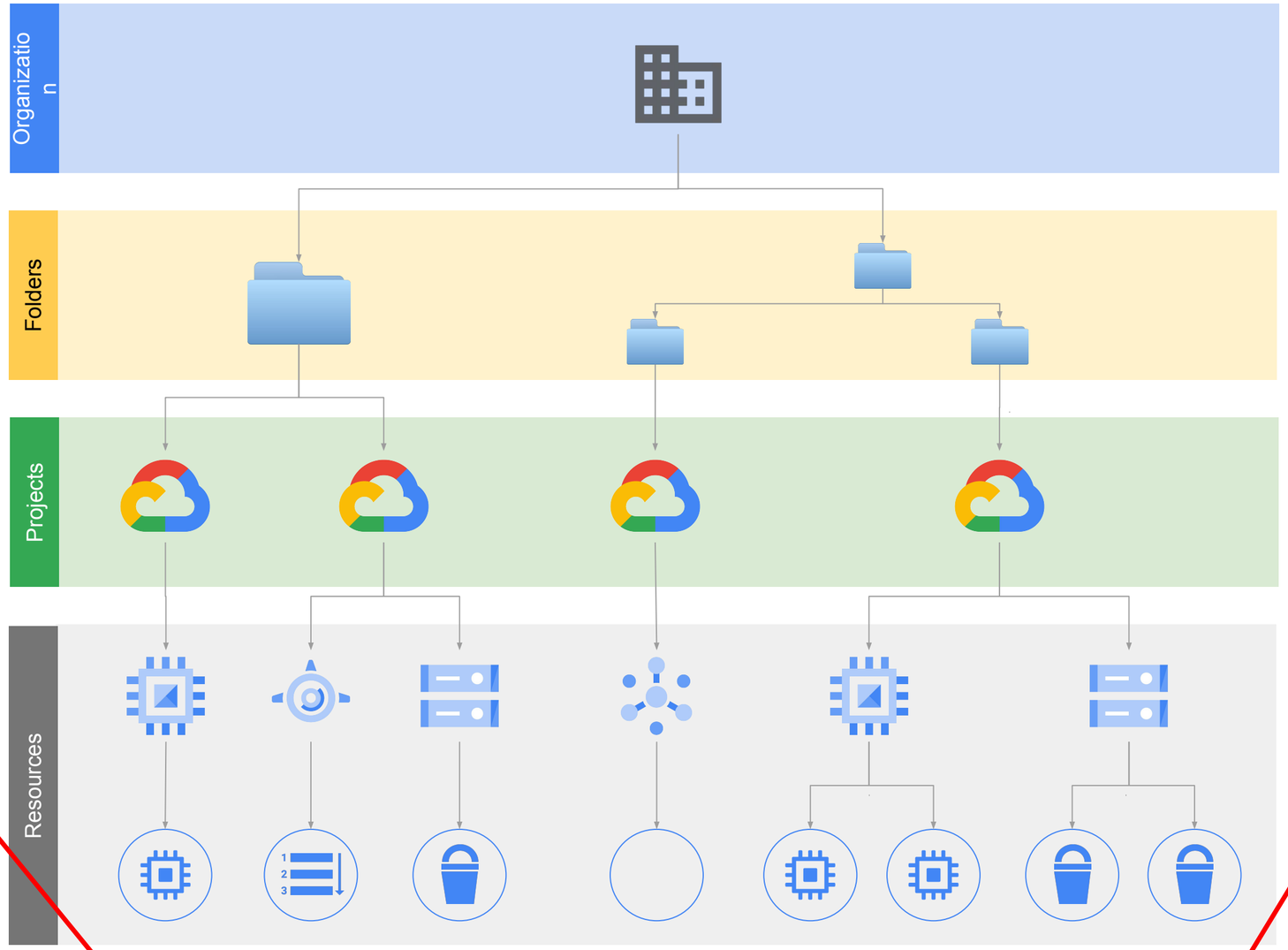
IAM

Hierarchy inheritance

IAM policy

Top-down inheritance

Additive only



Org Policy

Top-down inheritance

Allows overrides

Exam Tip: IAM Deny policies? Yes… and no…

IAM policy pattern example

inheritance

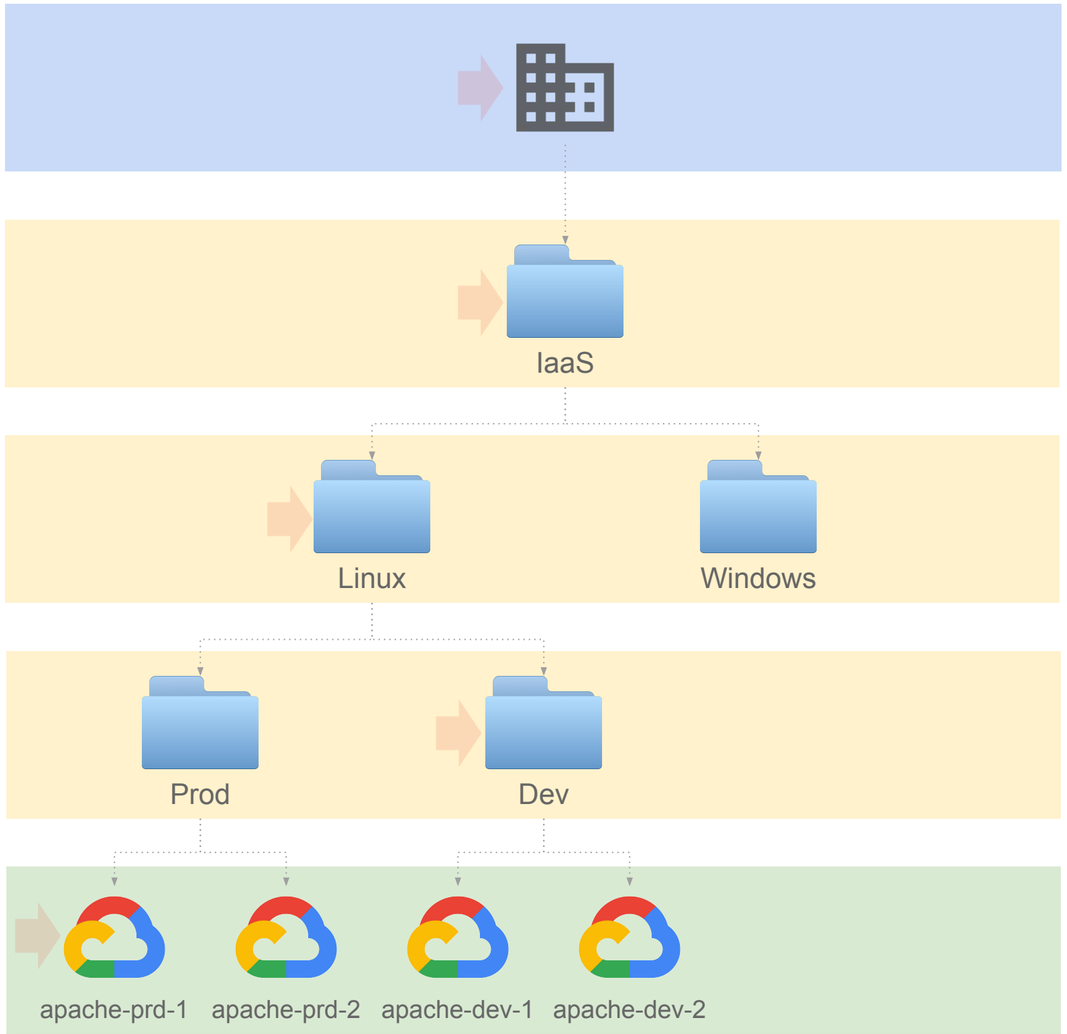
`roles/browser` → `domain:example.org`
all domain users should be able to see the hierarchy

`roles/viewer` → `group:first-lvl-support@`
support users should be able to view logs and VMs

`roles/compute.admin` → `group:linux-os@`
instance admins should manage resources

`roles/logging.logViewer` → `group:app-team-1@`
app admins should view logs in dev

`roles/storage.admin` → `serviceAccount:app1@`
ad-hoc permissions on project or single resource

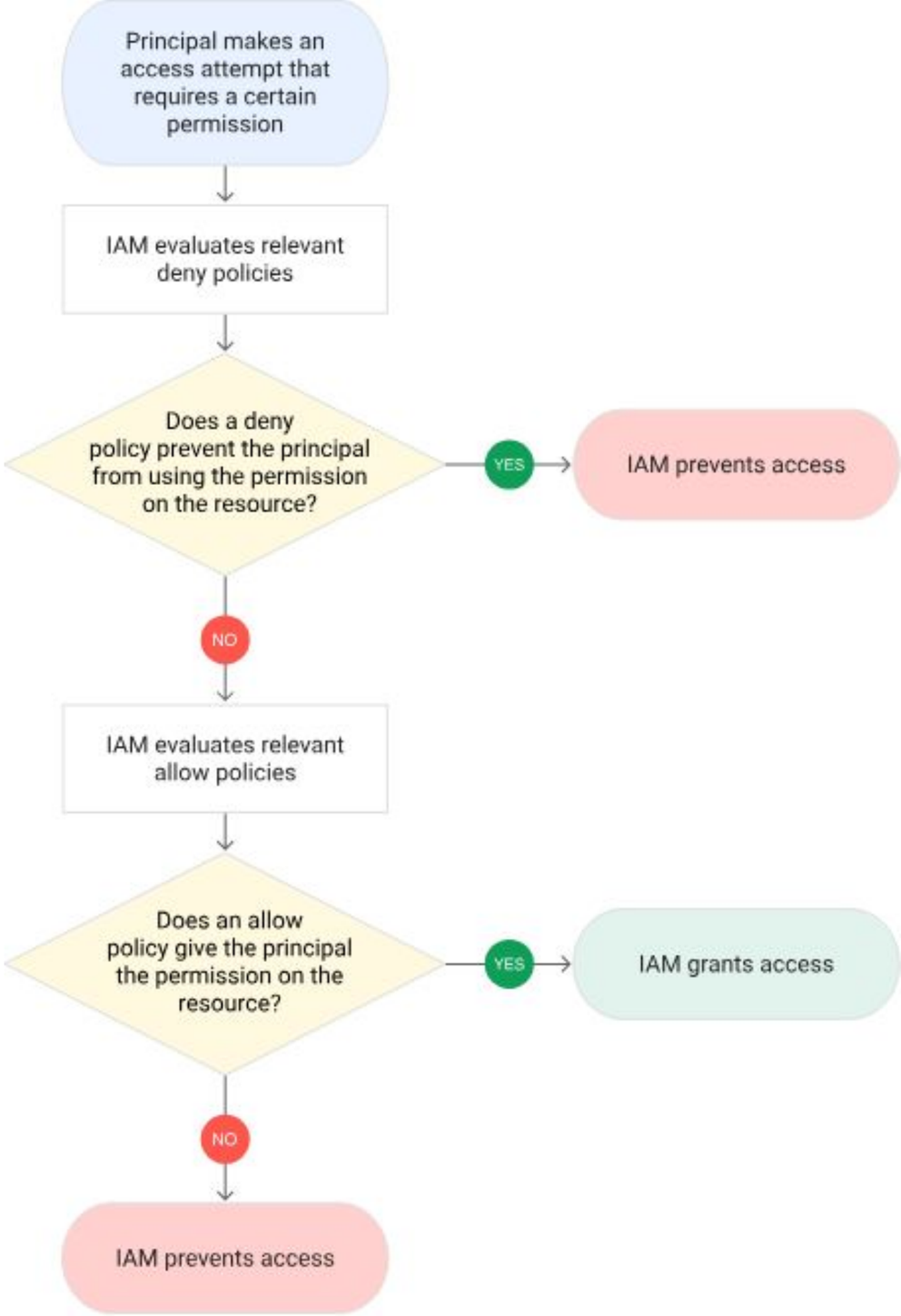


Organization Policy vs IAM Policy

Organization Policies	IAM Policies
Constraints that allow you to: ● Limit resource sharing based on domain. ● Limit the usage of Identity and Access Management service accounts. ● Restrict the physical location of newly created resources.	Effectively they're bindings which specify what access should be granted to principal on resources.
Focuses on "what". Allows to set restrictions on specific resources to determine how they can be configured	Focuses on "who". Let's you authorize who can take action on specific resources based on permissions
Can be set on different levels (org, folder, project), propagate down but lower-level policy overwrites a higher-level one.	Effective IAM Policy on each level is a SUM of all privileges (* with an exception of "deny policies", which are not covered on the exam as of Q1 '23)
Both should be used as part of a security posture! It's NOT one or the other.	

IAM DENY Policy

- You can define deny rules that prevent certain principals from using certain permissions, regardless of the roles they're granted, because IAM always checks relevant deny policies before checking relevant allow policies.
- To specify where you want a deny policy to apply, you attach it to a project, folder, or organization.
- For details, see here.



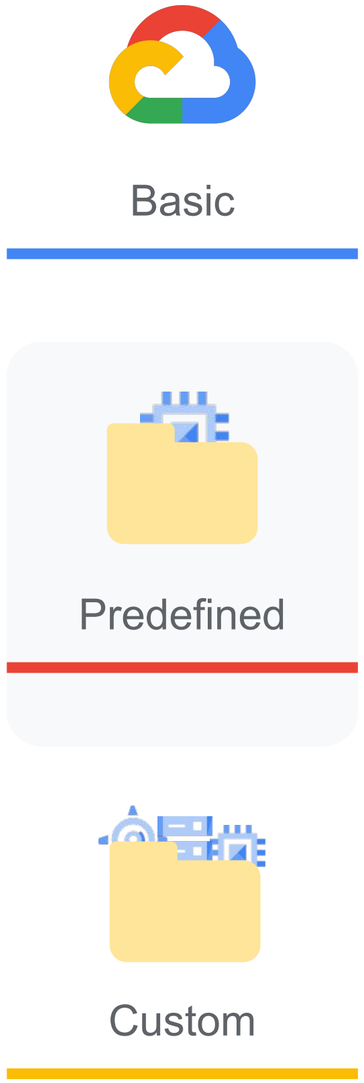
Bind roles to identities to provide access to resources

Roles are collections of permissions which align with the required access for an abstract job function

- Facilitate least privilege access control and separation of duties
- Can be bound at organization, folder, project, or resource level and flows downwards

Additional IAM-related services:

- Policy Simulator
- Policy Analyzer
- Policy Troubleshooter



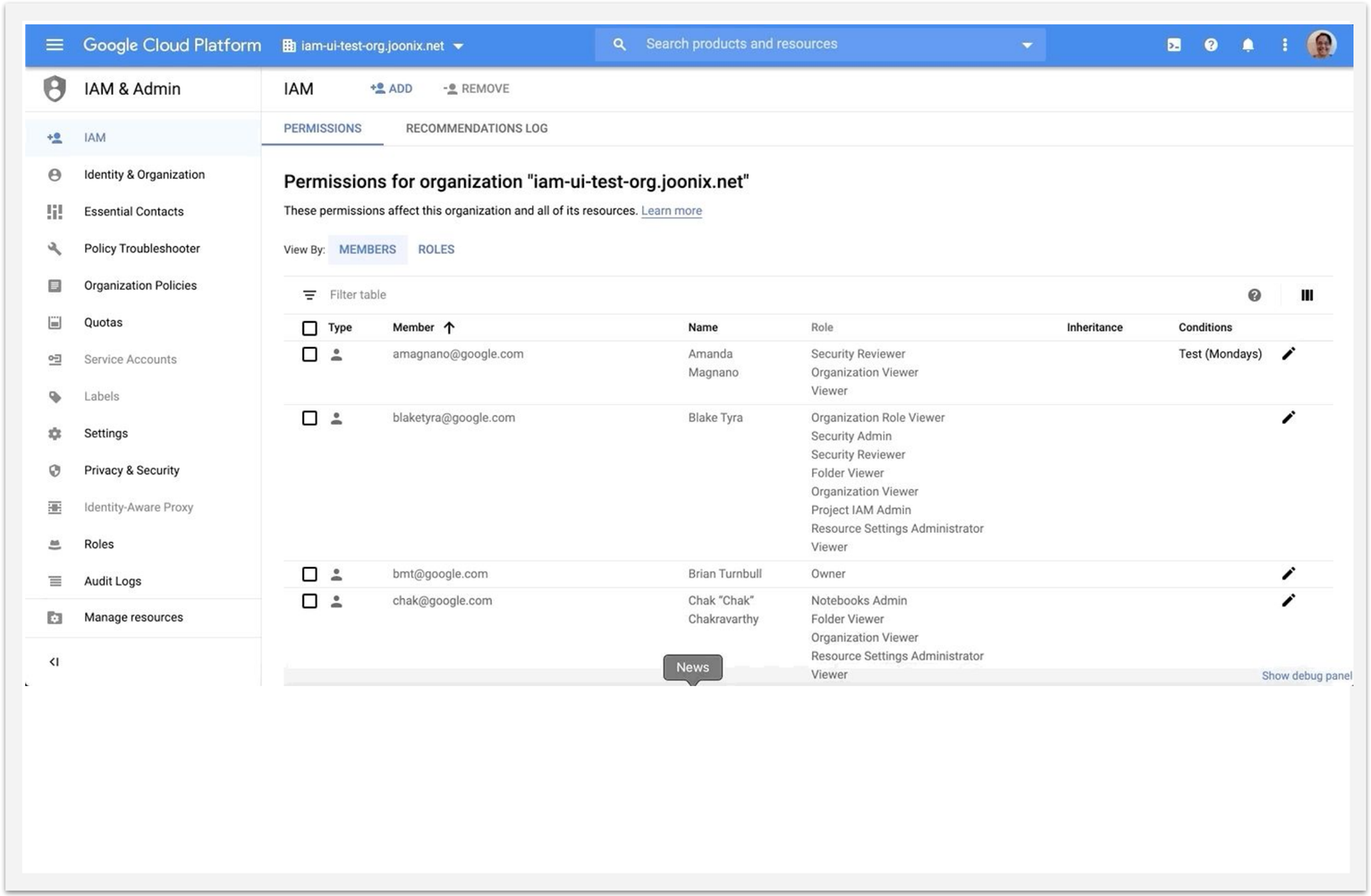
IAM Policy Simulator

Understand the impact of your policy changes **before** you make them.

But what if I break something?

Policy Simulator

- Simulate the impact of configuration changes



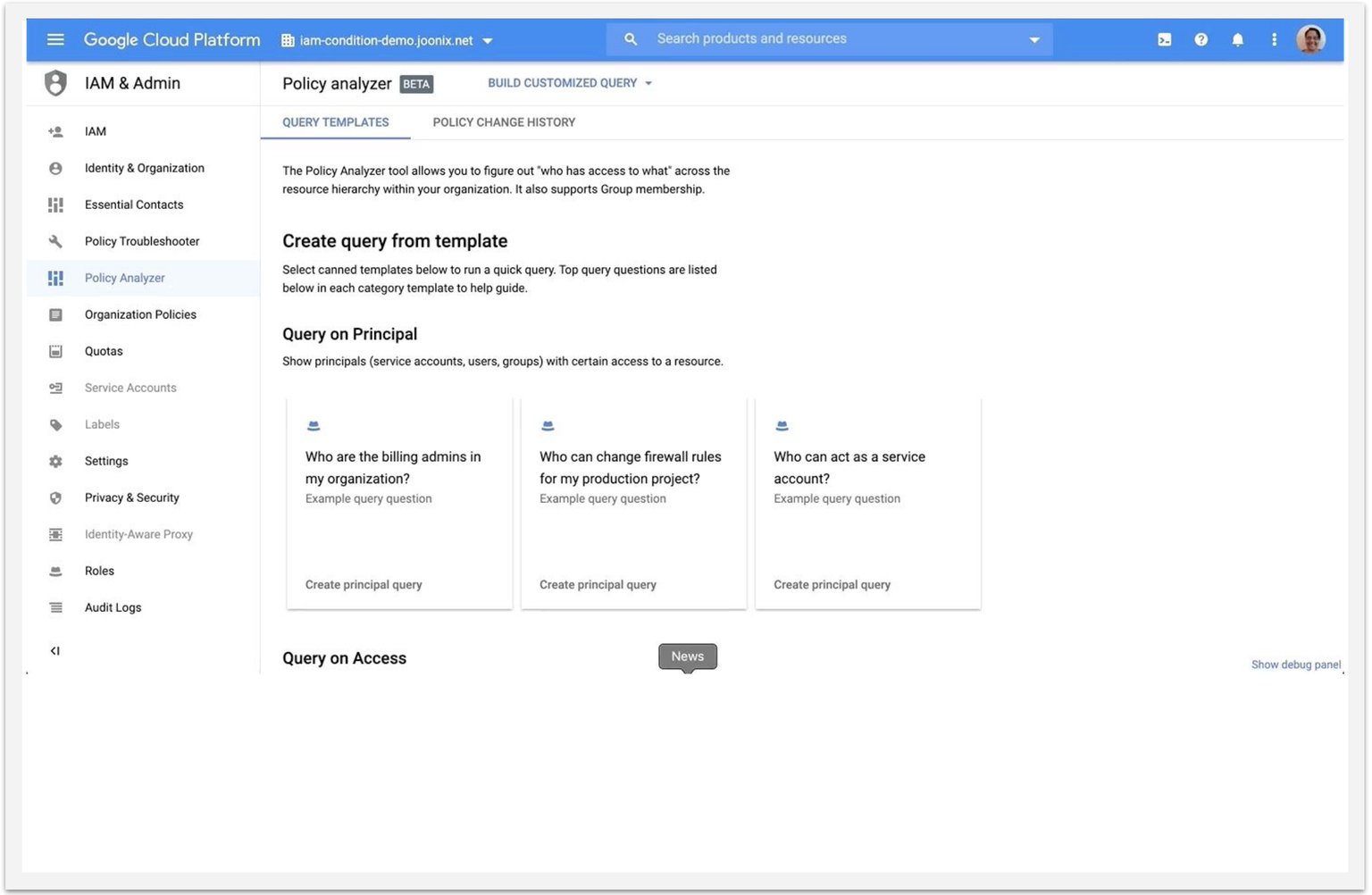
IAM Policy Analyzer

Understand who ***has access*** to which resources.

“Who has access to what?”

Policy Analyzer

- Understand who has access to resources and what they can do
- Easily query access and build ad-hoc reports



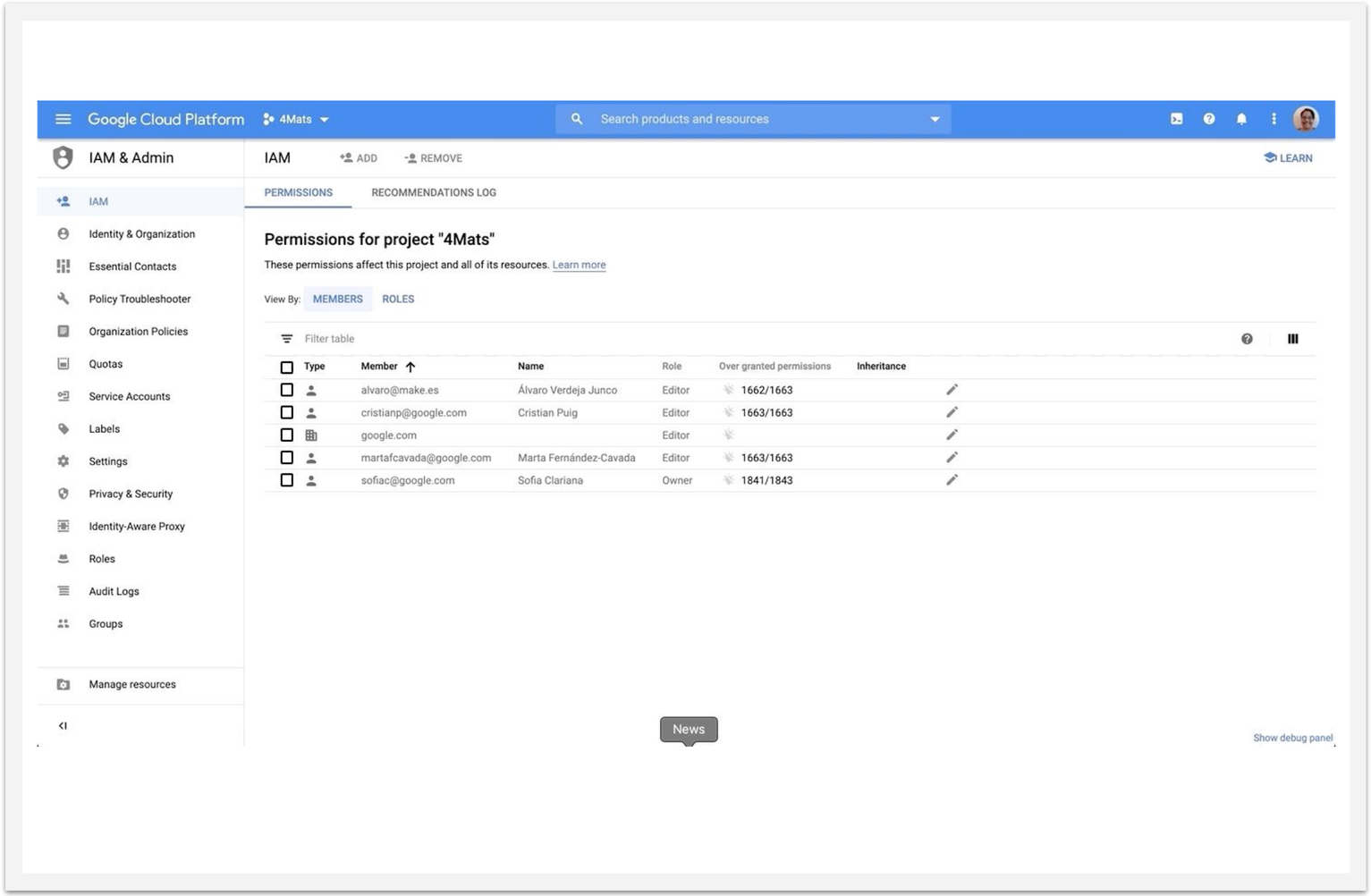
IAM Policy Troubleshooter

Explains why policies are preventing or allowing access.

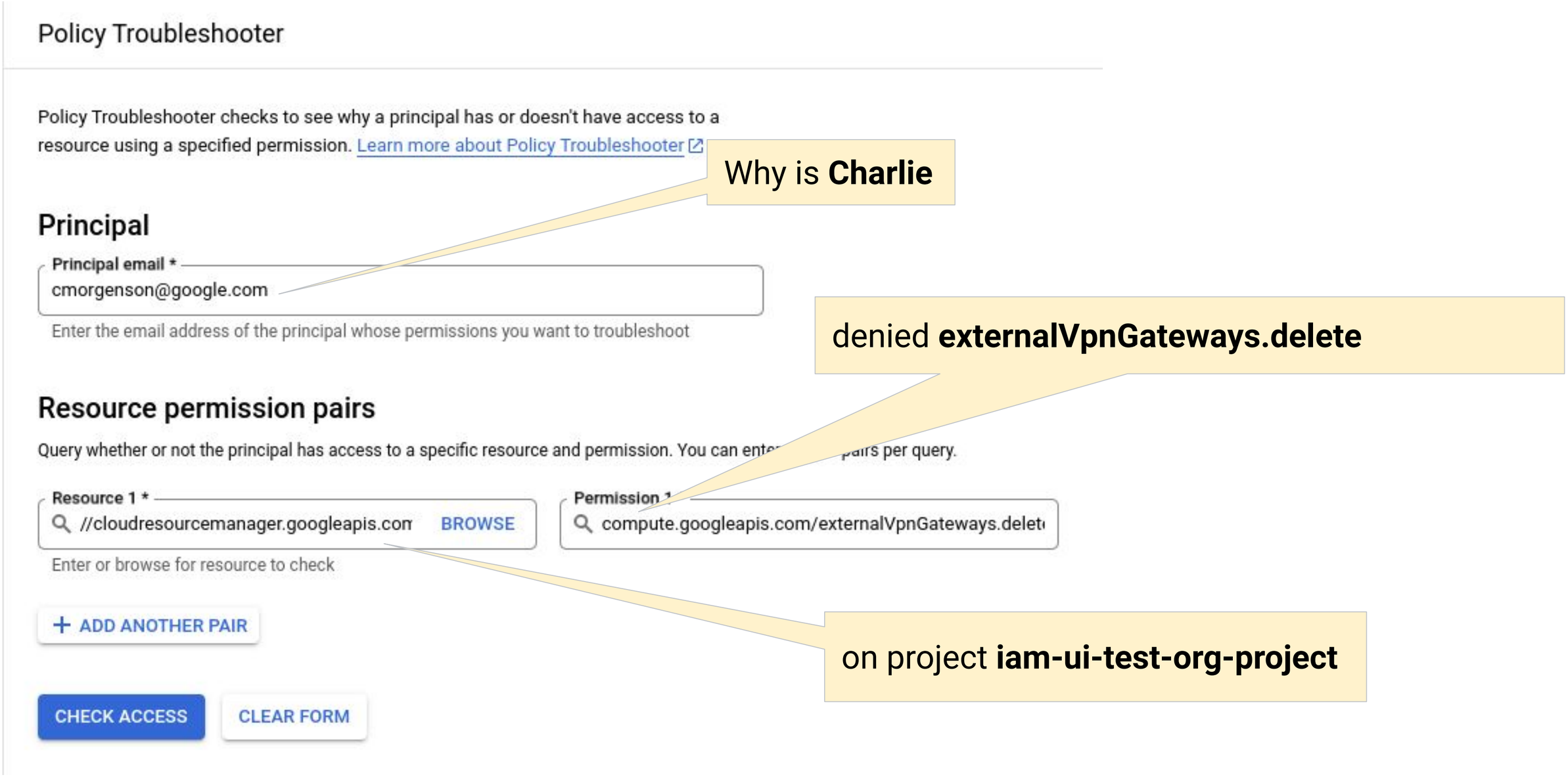
“My access is not working”

Policy Troubleshooter

- Understand why someone does not have access to a resource



Policy Troubleshooter



IAM Recommender

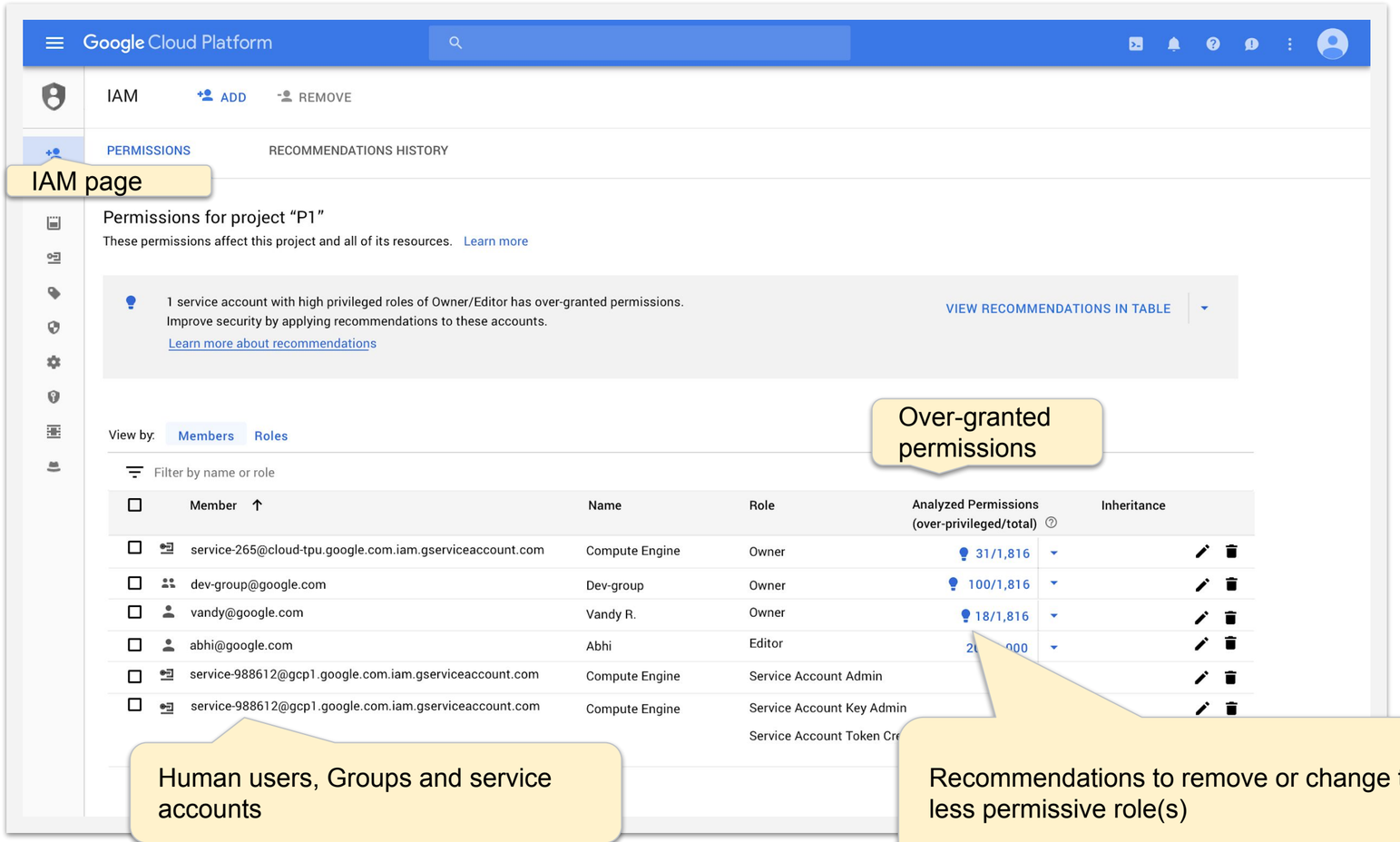
Reduce security risk by reducing IAM permission overgranting.

Least privilege at scale

3

IAM Recommender Now GA!

- Prescriptive guidance on how to reduce permissions to the minimal required set
- Based on historical activity
- Machine learning generated
- Identifies permissions that are safe to remove
- No config or setup required



IAM. Know how to…

- Create a custom IAM role (using YAML-file specification):

```
gcloud iam roles create ROLE_ID --project=PROJECT_ID \
    --file=YAML_FILE_PATH
```

- Get a list of permissions that are available for custom roles in a specific project or organization:

```
gcloud iam list-testable-permissions FULL_RESOURCE_NAME \
    --filter="customRolesSupportLevel!=NOT_SUPPORTED"
```

- Grant, change, and revoke access using gcloud command, such as:

```
gcloud RESOURCE_TYPE get-iam-policy RESOURCE_ID --format=FORMAT > PATH
```

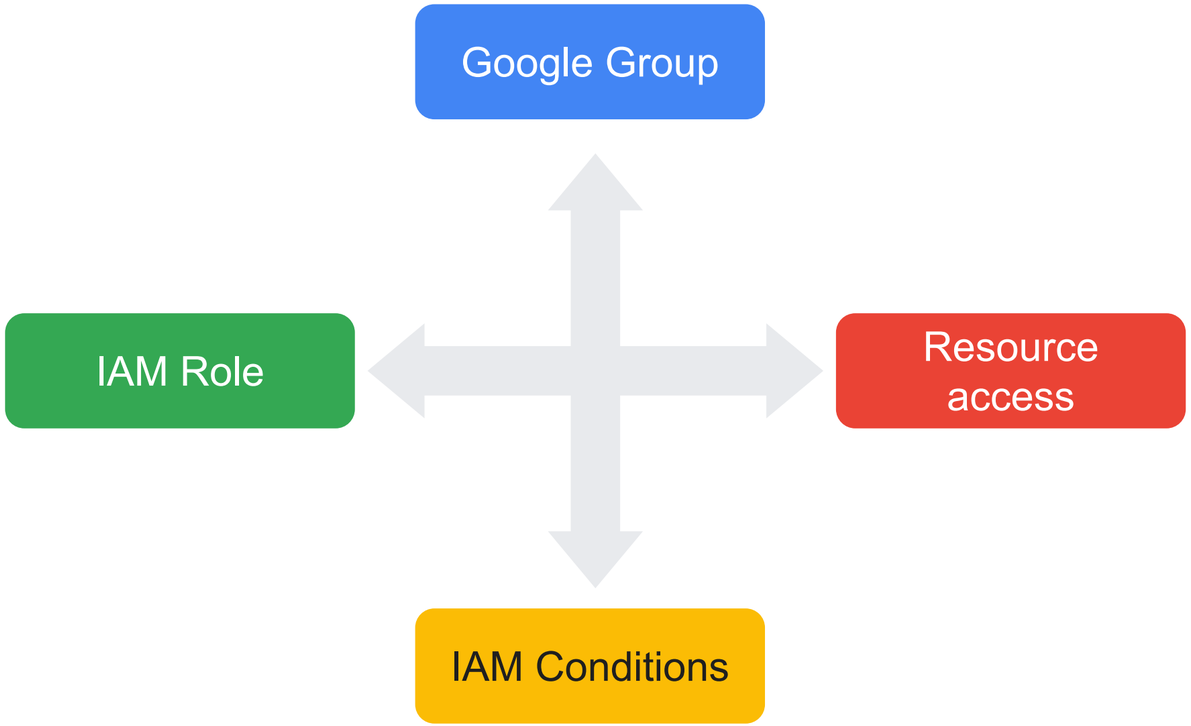
```
gcloud RESOURCE_TYPE set-iam-policy RESOURCE_ID PATH
```

```
gcloud RESOURCE_TYPE add-iam-policy-binding RESOURCE_ID \
    --member=PRINCIPAL --role=ROLE_ID \
    --condition=CONDITION
```

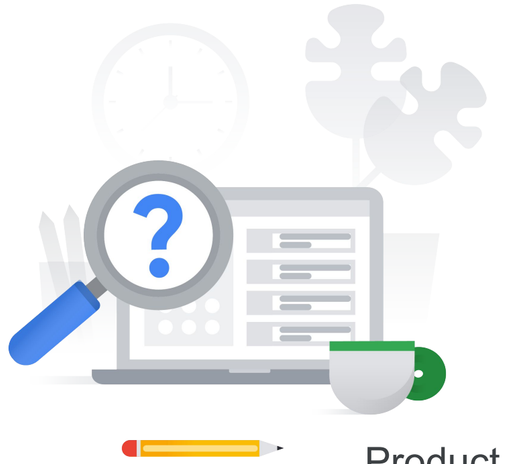
IAM conditions to control the where, when, how of access to resources

IAM conditions can be added to role bindings to control from where, when, and how the access can be used

- Allows for even better least privilege access control



1.5 Diagnostic Question 09 Discussion



Cymbal Bank is divided into separate departments. Each department is divided into teams. Each team works on a distinct product that requires Google Cloud resources for development.

How would you design a Google Cloud organization hierarchy to best match Cymbal Bank's organization structure and needs?

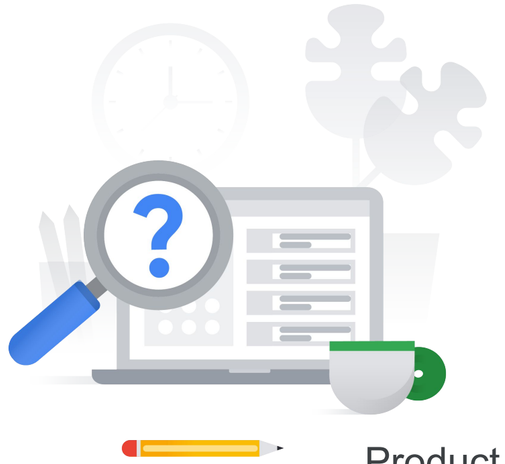
A. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Under each Product, create Teams folders. In the Teams folder, add Projects.

B. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Add Projects to the Product folders.

C. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Teams folders. Add Projects to the Teams folders.

D. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create a Teams folder. Under each Team, create Product folders. Add Projects to the Product folders.

1.5 Diagnostic Question 09 Discussion



Cymbal Bank is divided into separate departments. Each department is divided into teams. Each team works on a distinct product that requires Google Cloud resources for development.

How would you design a Google Cloud organization hierarchy to best match Cymbal Bank's organization structure and needs?

A. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Under each Product, create Teams folders. In the Teams folder, add Projects.

B. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Product folders. Add Projects to the Product folders.

C. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create Teams folders. Add Projects to the Teams folders.

D. Create an Organization node. Under the Organization node, create Department folders. Under each Department, create a Teams folder. Under each Team, create Product folders. Add Projects to the Product folders.

1.4 Diagnostic Question 07 Discussion

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. Each product folder contains one Google Cloud Project, but more may be added. Each project contains an App Engine deployment.

Cymbal Bank has hired a new technical product manager and a new web developer. The technical product manager must be able to interact with and manage all services in projects that roll up to the Engineering Department folder. The web developer needs read-only access to App Engine configurations and settings for a specific product.

How should you provision the new employees' roles into your hierarchy following principles of least privilege?

A. Assign the Project Editor role in each individual project to the technical product manager. Assign the Project Editor role in each individual project to the web developer.

B. Assign the Project Owner role in each individual project to the technical product manager. Assign the App Engine Deployer role in each individual project to the web developer.

C. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Assign the App Engine Deployer role at the specific product's folder level to the web developer.

D. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Create a Custom Role in the product folder that the web developer needs access to. Add the appengine.versions.create and appengine.versions.delete permissions to that role, and assign it to the web developer.

1.4 Diagnostic Question 07 Discussion

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. Each product folder contains one Google Cloud Project, but more may be added. Each project contains an App Engine deployment.

Cymbal Bank has hired a new technical product manager and a new web developer. The technical product manager must be able to interact with and manage all services in projects that roll up to the Engineering Department folder. The web developer needs read-only access to App Engine configurations and settings for a specific product.

How should you provision the new employees' roles into your hierarchy following principles of least privilege?

A. Assign the Project Editor role in each individual project to the technical product manager. Assign the Project Editor role in each individual project to the web developer.

B. Assign the Project Owner role in each individual project to the technical product manager. Assign the App Engine Deployer role in each individual project to the web developer.

C. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Assign the App Engine Deployer role at the specific product's folder level to the web developer.

D. Assign the Project Editor role at the Engineering Department folder level to the technical product manager. Create a Custom Role in the product folder that the web developer needs access to. Add the appengine.versions.create and appengine.versions.delete permissions to that role, and assign it to the web developer.

5.2 Diagnostic Question 07 Discussion

Cymbal Bank needs to do an analysis to verify which users and groups have been given the Network Admin role for a particular VPC network.

Select the simplest setup and process to accomplish this.

A. Use the Policy Troubleshooter to test each user and group against the VPC and each of the permissions in the Network Admin role.

A. Use the Policy Simulator to simulate providing the Network Admin role to each user and group. Review the results to determine which identities would have access changes.

A. Use the Policy Analyzer with scope set to Organization, and resource set to the VPC, and role set to Network Admin.

A. Use the Policy Analyzer with scope set to Organization, resource set to the VPC, role set to Network Admin, and identity set to all users and groups.

5.2 Diagnostic Question 07 Discussion

Cymbal Bank needs to do an analysis to verify which users and groups have been given the Network Admin role for a particular VPC network.

Select the simplest setup and process to accomplish this.

A. Use the Policy Troubleshooter to test each user and group against the VPC and each of the permissions in the Network Admin role.

A. Use the Policy Simulator to simulate providing the Network Admin role to each user and group. Review the results to determine which identities would have access changes.

A. Use the Policy Analyzer with scope set to Organization, and resource set to the VPC, and role set to Network Admin.

A. Use the Policy Analyzer with scope set to Organization, resource set to the VPC, role set to Network Admin, and identity set to all users and groups.

1.3 Diagnostic Question 06 Discussion

Cymbal Bank's Mobile Development Team has an AI Platform instance in a Google Cloud Project. An auditor needs to record the AI Platform jobs and models, along with their usage. You need to assign permissions to the external auditors so that they can view the models and jobs but not retrieve specific details on any of them.

What should you do?

A. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions ml.models.list and ml.jobs.list. Use `gIAM roles create role-id -- organization organization-id --file=json-file-path.`

B. Create a custom role for auditors at the Project level. Create a YAML file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id --project project-id --file=yaml-file-path.`

C. Create a custom role for auditors at the Project level. `Use gIAM roles create role-name --project project-id --permissions= ml.models.get, ml.jobs.get.`

D. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM role create role-id --organization organization-id --file=json-file-path.`

1.3 Diagnostic Question 06 Discussion

Cymbal Bank's Mobile Development Team has an AI Platform instance in a Google Cloud Project. An auditor needs to record the AI Platform jobs and models, along with their usage. You need to assign permissions to the external auditors so that they can view the models and jobs but not retrieve specific details on any of them.

What should you do?

A. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions ml.models.list and ml.jobs.list. Use `gIAM roles create role-id -- organization organization-id --file=json-file-path.`

B. Create a custom role for auditors at the Project level. Create a YAML file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM roles create role-id --project project-id --file=yaml-file-path.`

C. Create a custom role for auditors at the Project level. Use `gIAM roles create role-name --project project-id --permissions= ml.models.get, ml.jobs.get.`

D. Create a custom role for auditors at the Organization level. Create a JSON file with required permissions `ml.models.list` and `ml.jobs.list`. Use `gIAM role create role-id --organization organization-id --file=json-file-path.`

1.4 Diagnostic Question 08 Discussion

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. One folder titled "analytics" contains a Google Cloud Project that contains an App Engine deployment and a Cloud SQL instance.

A team needs specific access to this project. The team lead needs full administrative access to App Engine and Cloud SQL. A developer must be able to configure and manage all aspects of App Engine deployments. There is also a code reviewer who may periodically review the deployed App Engine source code without making any changes.

What types of permissions would you provide to each of these users?

A. Create custom roles for all three user types at the "analytics" folder level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

B. Assign the basic 'App Engine Admin' and 'Cloud SQL Admin" roles to the team lead. Assign the 'App Engine Admin' role to the developer. Assign the 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the analytics project level.

C. Create custom roles for all three user types at the project level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

D. Assign the basic 'Editor' role to the team lead. Create a custom role for the developer. Provide all appengine.* permissions to the developer. Provide the predefined 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the "analytics" folder level.

1.4 Diagnostic Question 08 Discussion

Cymbal Bank's organizational hierarchy divides the Organization into departments. The Engineering Department has a 'product team' folder. This folder contains folders for each of the bank's products. One folder titled "analytics" contains a Google Cloud Project that contains an App Engine deployment and a Cloud SQL instance.

A team needs specific access to this project. The team lead needs full administrative access to App Engine and Cloud SQL. A developer must be able to configure and manage all aspects of App Engine deployments. There is also a code reviewer who may periodically review the deployed App Engine source code without making any changes.

What types of permissions would you provide to each of these users?

A. Create custom roles for all three user types at the "analytics" folder level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

B. Assign the basic 'App Engine Admin' and 'Cloud SQL Admin" roles to the team lead. Assign the 'App Engine Admin' role to the developer. Assign the 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the analytics project level.

C. Create custom roles for all three user types at the project level. For the team lead, provide all appengine.* and cloudsql.* permissions. For the developer, provide appengine.applications.* and appengine.instances.* permissions. For the code reviewer, provide the appengine.instances.* permissions.

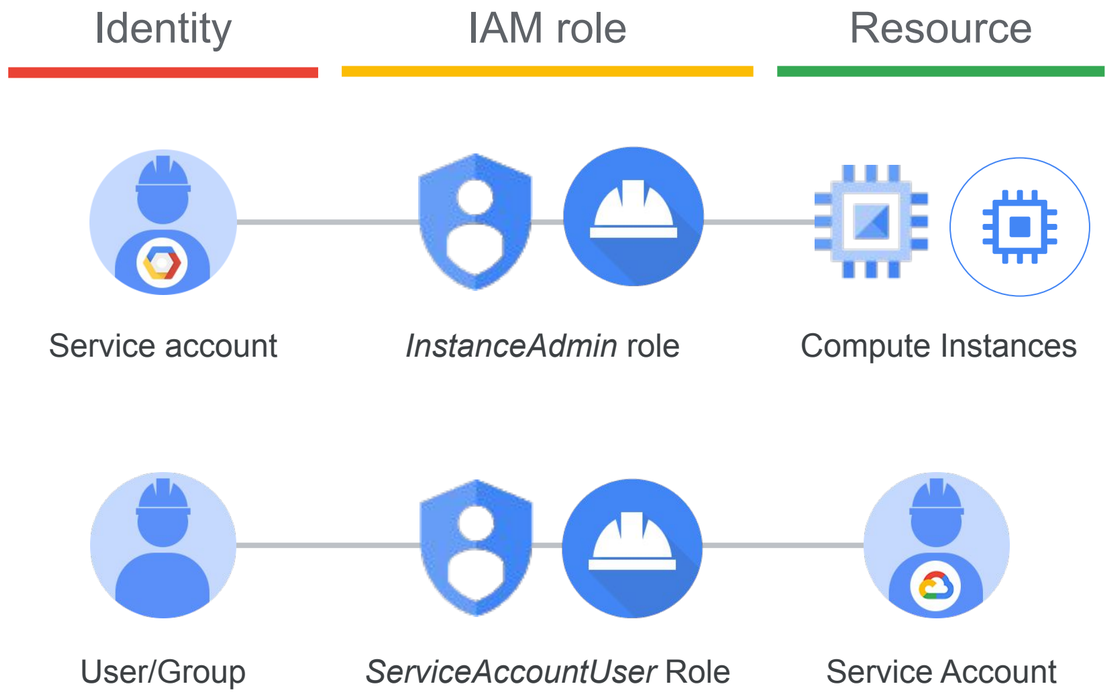
D. Assign the basic 'Editor' role to the team lead. Create a custom role for the developer. Provide all appengine.* permissions to the developer. Provide the predefined 'App Engine Code Viewer' role to the code reviewer. Assign all these permissions at the "analytics" folder level.

Service Accounts

Service accounts provide service access to Google Cloud

Service accounts used as service identities for workloads running in or outside Google Cloud

- Given access to resources like user and group identities
- Authenticate with private keys
- Leverage Google key management for most secure usage



Exam Tips:

- *Have a look at* Service Account recommendations
- Make sure to understand Service Account impersonation.

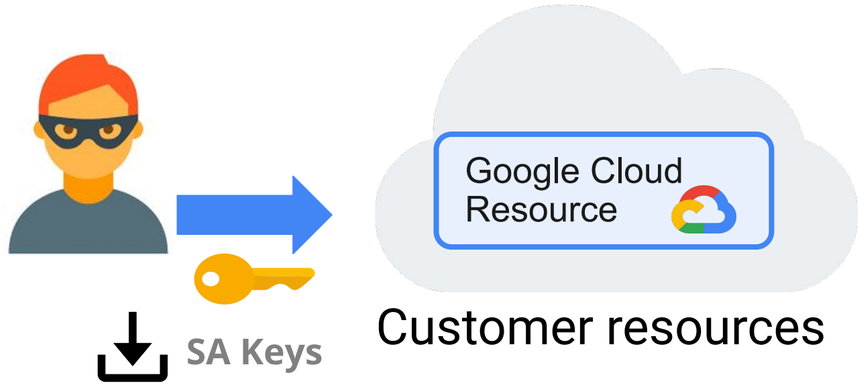
Service account keys recommendations

- Not recommended to generate SA keys at all if not absolutely needed. What are the alternatives?
  - Workload Identity
  - Workload Identity Federation
  - Short-lived credentials
- Limit projects where you can create Service Accounts / Service Account keys.
- Don't keep keys in source code repos / program binaries
- Don't store keys in Secret Manager! It's for secrets, not encryption keys
- If you generated the public/private key pair yourself, stored the private key in a hardware security module (HSM), and uploaded the public key to Google.
- etc…

All Service Account keys recommendations

Service account (SA) keys pose a security risk to your cloud resources

- SA keys are similar to a **password without an expiration date**.
- SA Keys can be leaked accidently and attackers can use it to access your (GCP project or org admin) sensitive GCP resources.
- Usage cannot be audited → compounding the risk



Customers have downloaded > 48 Million Service Account Keys!!

So what's the solution? Ditch the keys and use Workload Identity & Workload Identity Federation!

Workload Identity Federation: Keyless Access

User Story: As an App Developer, I want to **securely connect my services (= NOT users, like in Workforce Identity Federation!)** to GCP resources without downloading access keys.

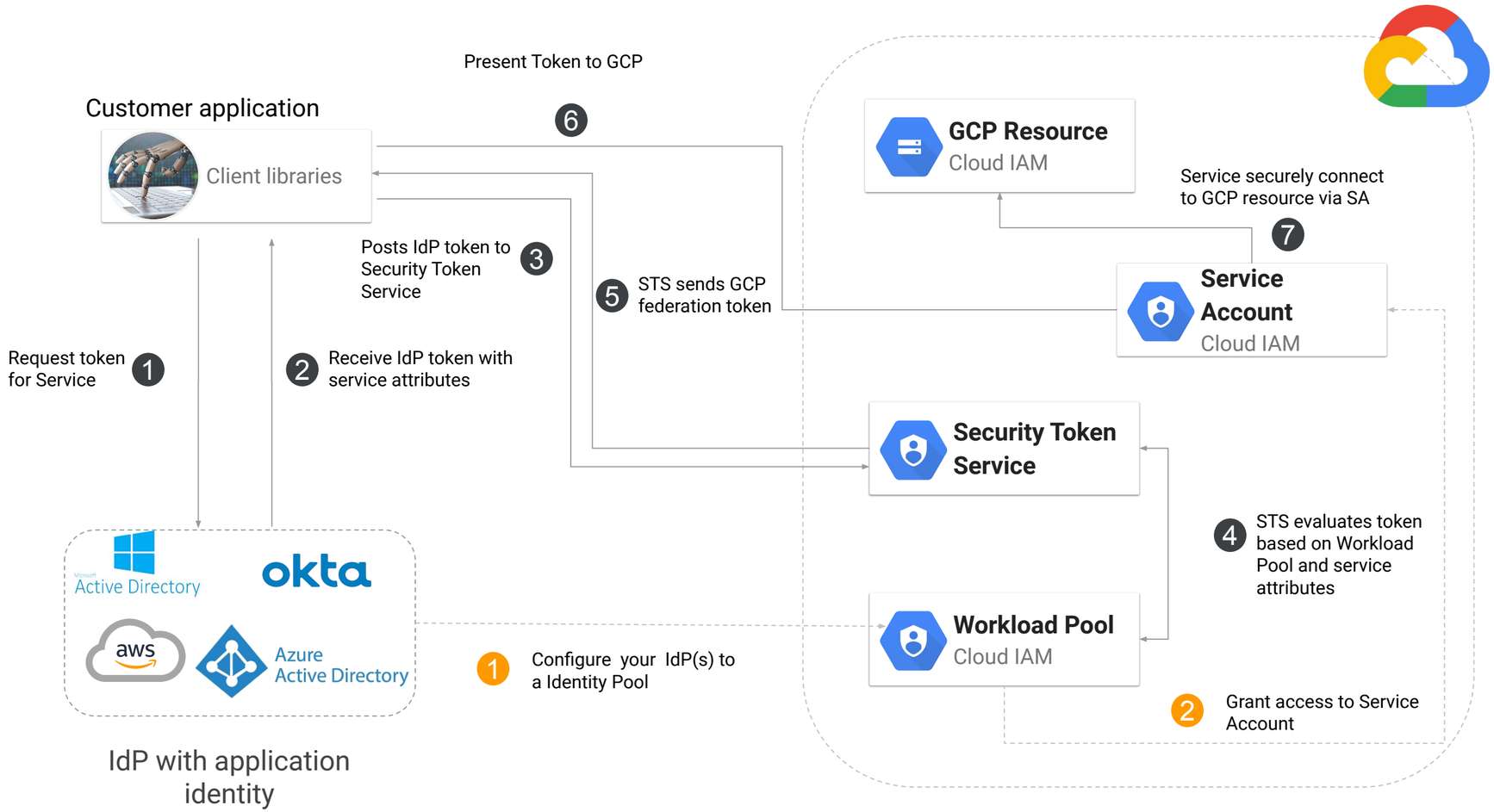
Benefits

Keyless access to GCP APIs

Auditability through Cloud logs

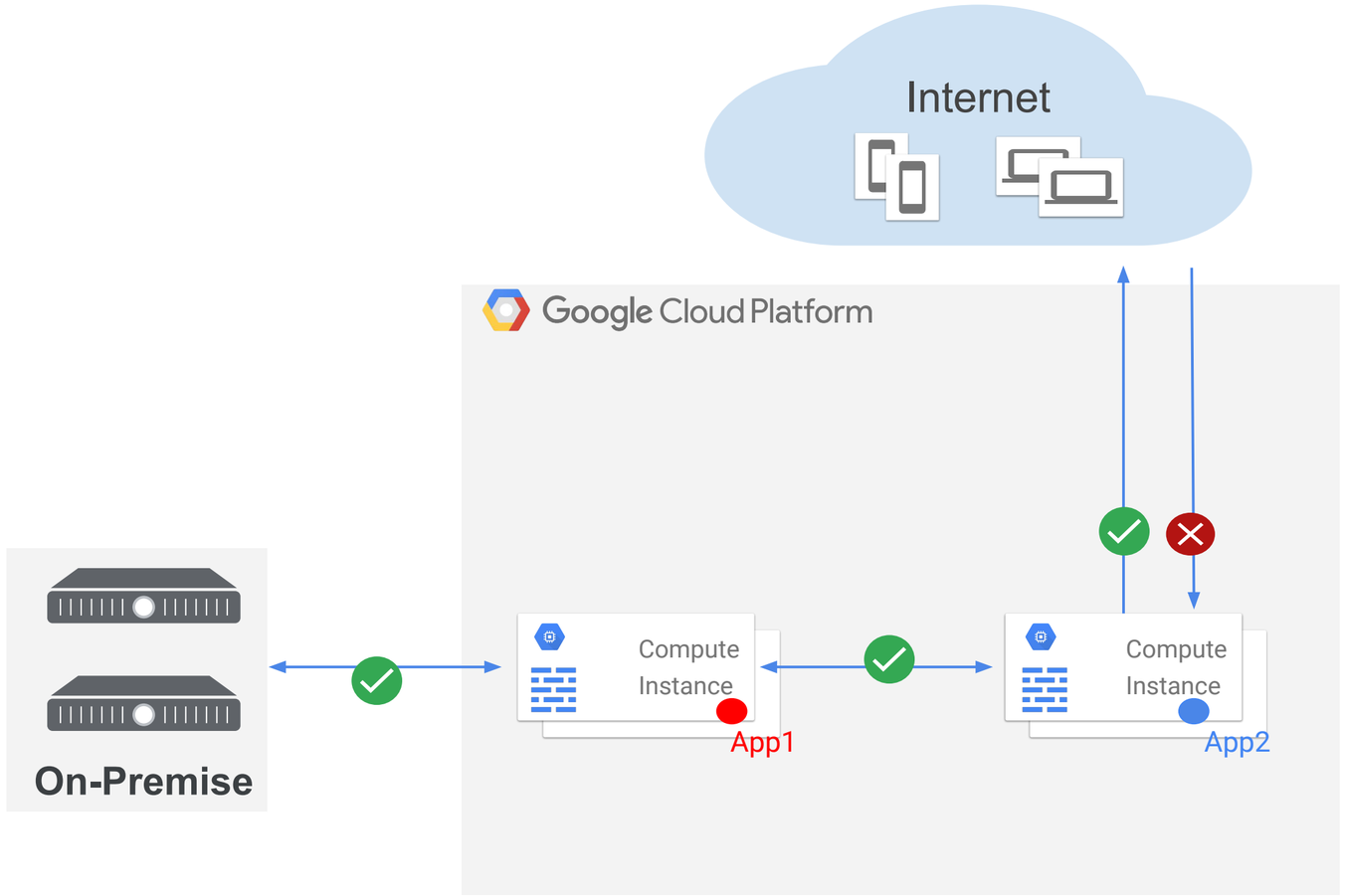
Attribute-based access control

Exam Tip: Have a look at a great explanation of WIF.



Firewall

Google Cloud Firewall

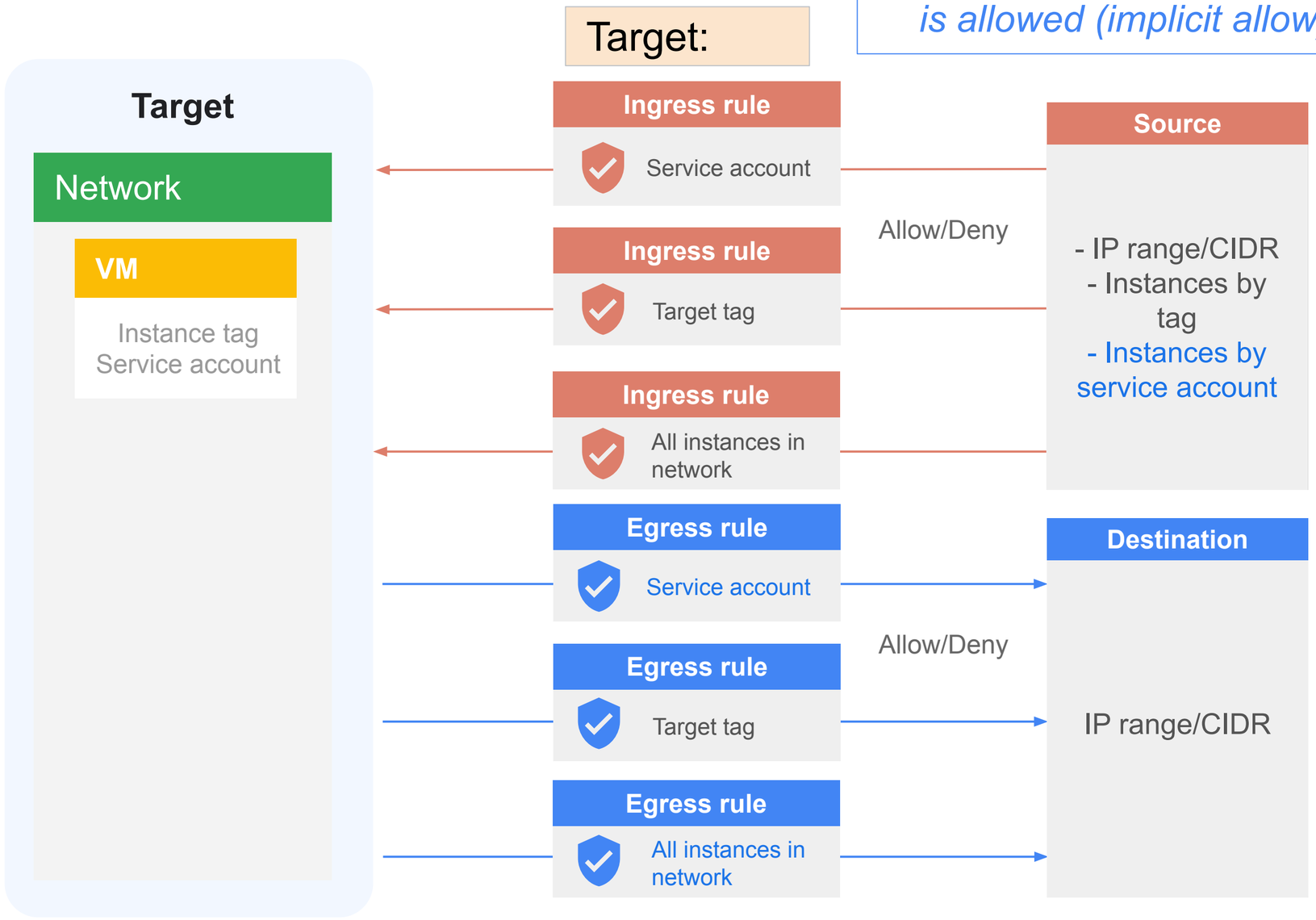


1. Fully distributed host-based enforcement
2. Ingress and egress access control
3. Stateful connection tracking
4. Microsegmentation with network tags and service accounts

VPC firewall rules

Exam Tips:

- *Default priority = 1000, lower value is higher priority.*
- *In a new VPC: All Ingress is blocked (implicit deny), all Egress is allowed (implicit allow)*



VPC firewall

- **Stateful** with connection tracking
- **Distributed**: enforced on underlying host

Controls paths

- VM <-> VM
- VM <-> Internet
- VM <-> On-prem

Implied rules

- Ingress deny
- Egress allow

Attaching firewall rules to VMs

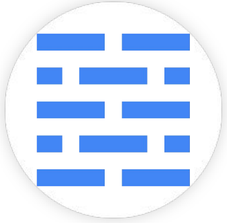
Tags

- Multiple tags applied to one VM (64 max)
- Firewall rule may target multiple tags
- May update tags to live VM

Best practice

Service accounts

- May restrict who uses
- Must shut down VM to change service account

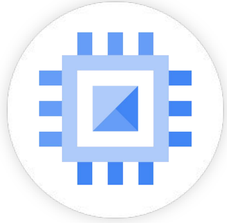


Firewall rule

Rule applied to service account

Service account

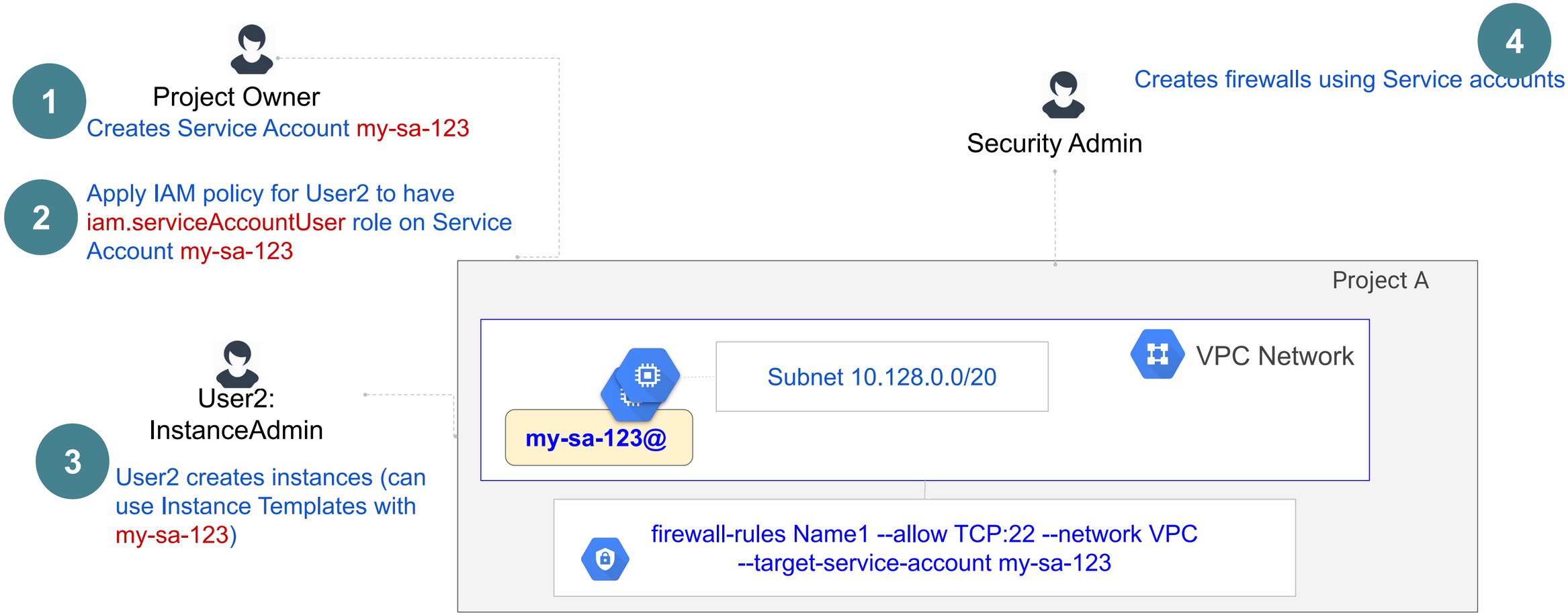
Service account compute identity



Compute instance

Firewall Rules based on Service Accounts

- Tags are inherently unsafe (cannot be ACL'd)
- Service Accounts are VM identities and are subject to IAM permission checks

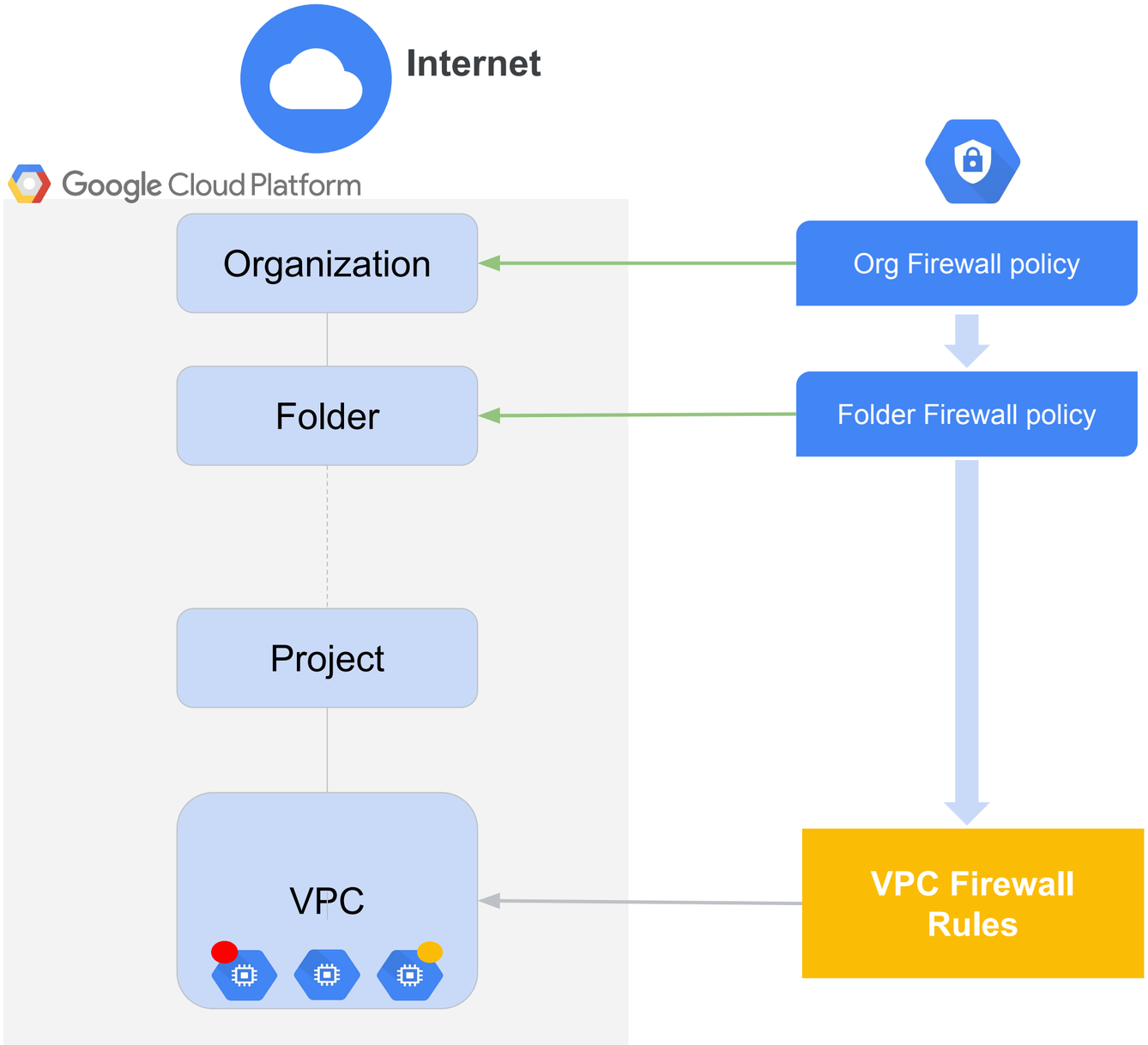


Hierarchical Firewall Policies

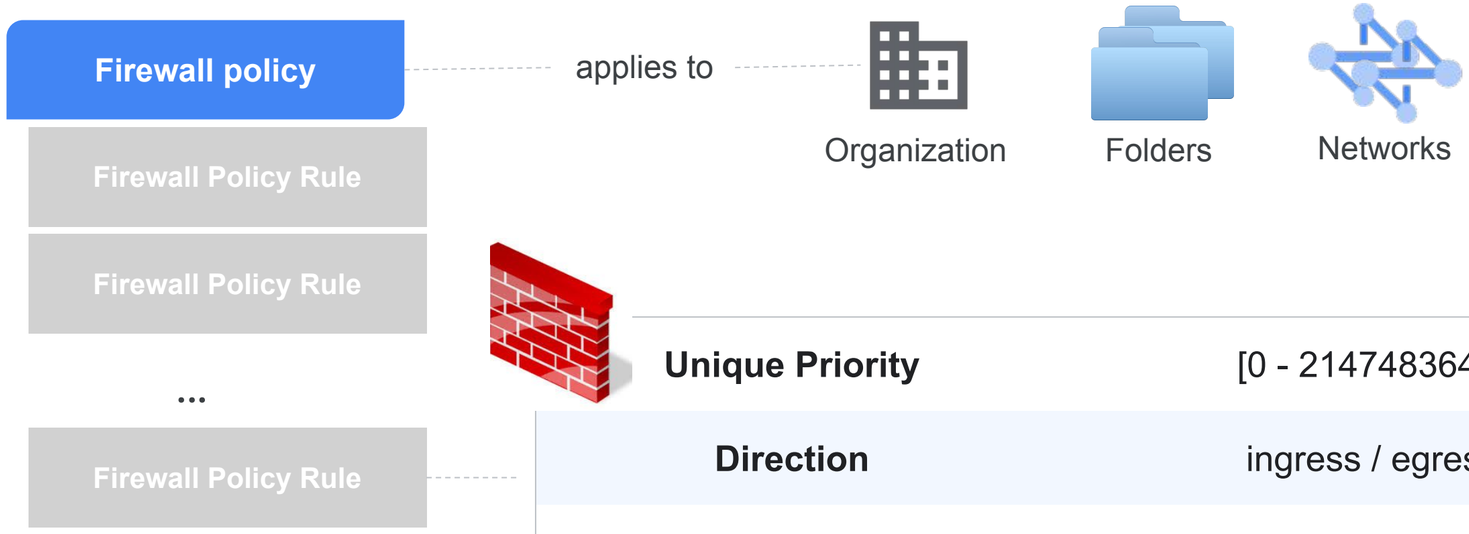
(yeah… another policy…)

Secure & Flexible Protection for Your Dynamic Cloud Environment

1. **Firewall Policies** containing multiple firewall rules as a single object attachable to Organization and Folders
2. **Hierarchical** policy enforcement enables safe delegation and automatic protection of new projects and networks
3. **Flexible** firewall target configuration supports the need for complex cloud deployment protection



Firewall Policies Anatomy



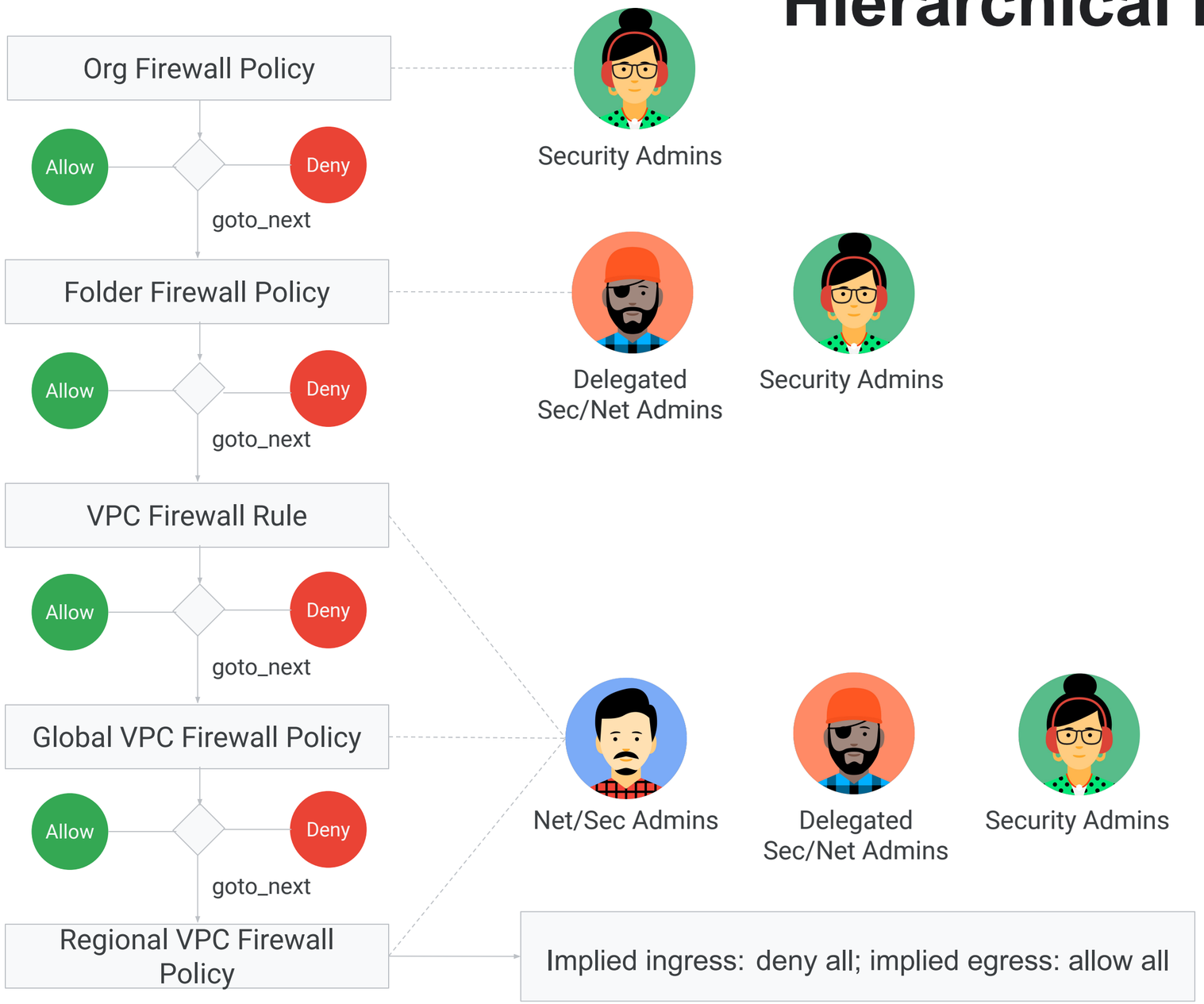
Unique Priority	[0 - 2147483643]
Direction	ingress / egress
Action	allow / deny / goto_next
Source / Destination Filters	IPv4 / IPv6 / secure tags (* i)
Target Type	All instances / service accounts / secure tags (*)
Protocols and Ports	port:protocol

(*) applies to network firewall policies only

(i) applies to Ingress rules only

- Firewall policy rules **are not VPC firewall rules**
- Within firewall policies, **rules are evaluated in order**.
  Lower numbers prioritized first
- Create network firewall policies under project node. Firewall policies can be attached to multiple VPCs within **same** project.
- **One firewall policy per VPC** (if global). The control/config object of this policy is stored globally
- **One firewall policy per VPC, per region** (if regional). The control/config object of this policy is stored regionally thereby enabling compliance requirements.

Hierarchical Policy Deployment



- Firewall policies are **hierarchical**
- Policies can attach to multiple resource hierarchy nodes
- **Inheritance is top down**, from the organization to the single VPCs
- Security admins can enforce company-wide policies or safely delegate
- At each level, three **actions**
  - allow
  - deny
  - goto_next(in hierarchy)

Firewall Policy vs. VPC Firewall Rules

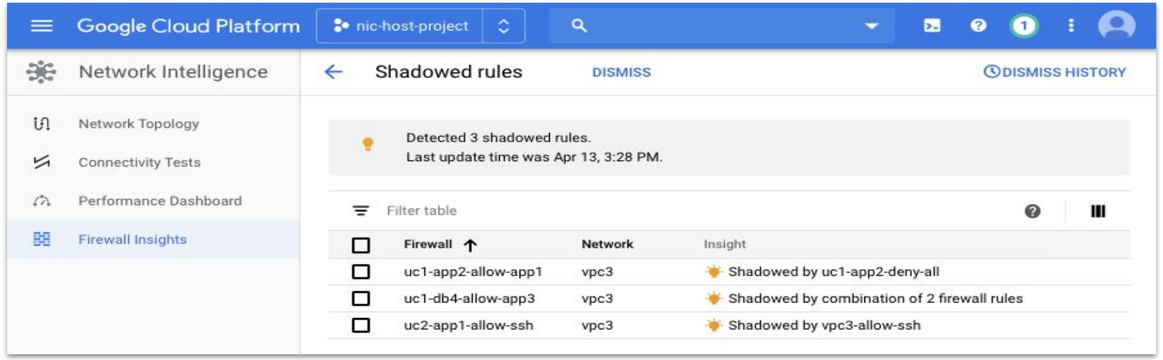
Rules in Firewall Policies are similar to VPC Firewall Rules with a few differences:

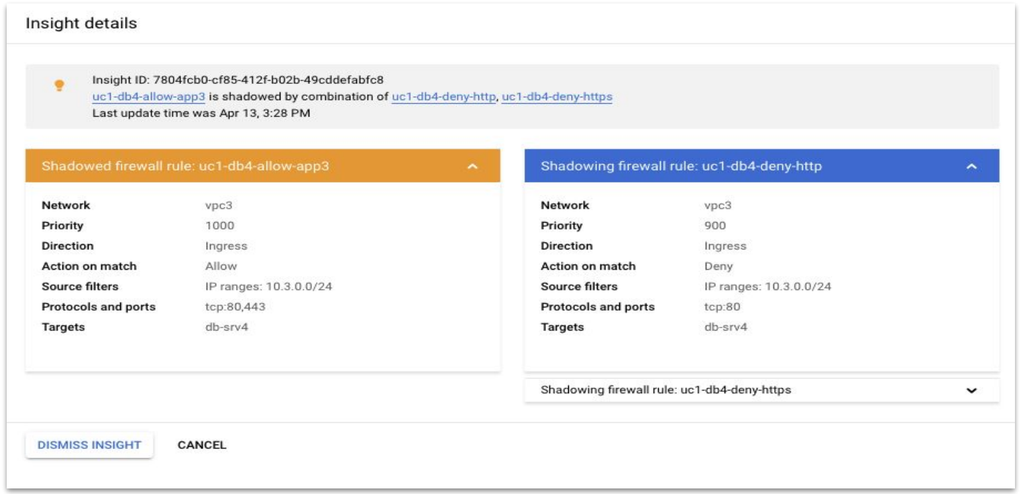
	VPC Firewall Rules	Firewall Policy Rules
Action Supported	Allow/deny	Allow/deny/**goto_next**
Service Account	Yes	**Target** only
Network Tag	Yes	**No**
Rule Name	mandatory	optional
Quota	Rule count	**Attribute** count
Priority	Duplication allowed	**No duplication** allowed

Firewall Insights

Misconfigured Firewall Rules

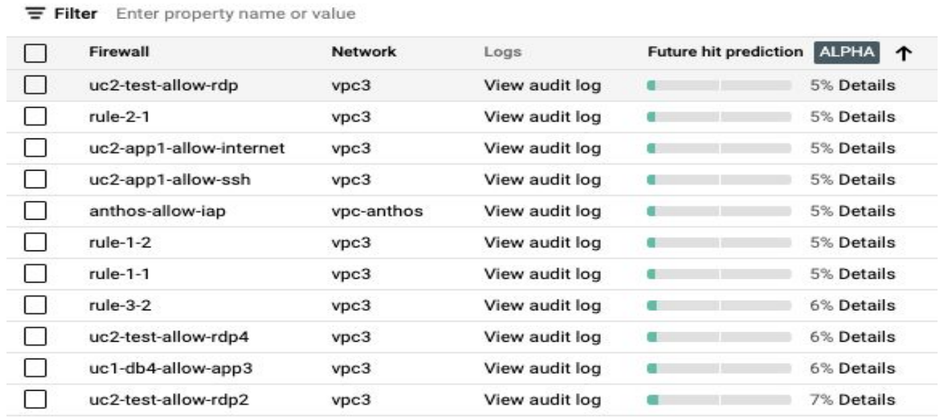
Shadowed Rule Detection (based on configuration analysis)

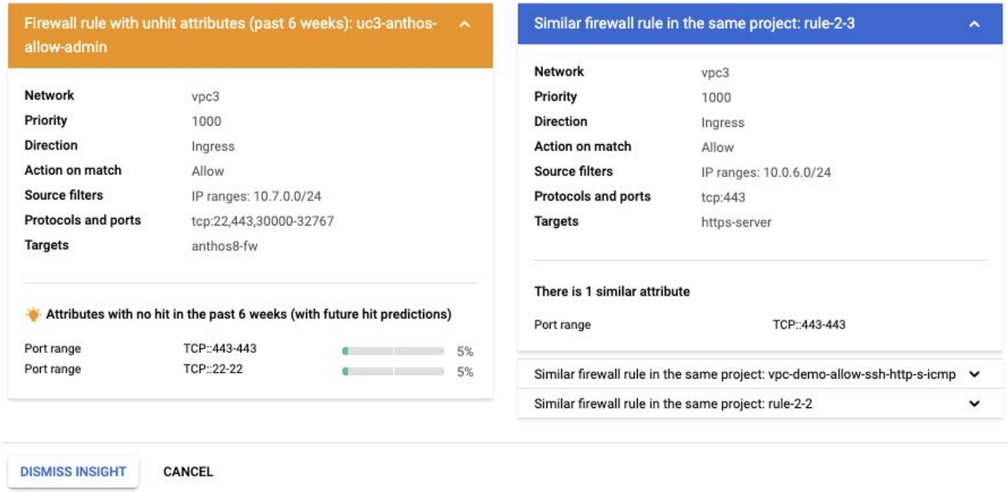




Usage Metrics & Overly Permissive Rules

(based on firewall log analysis)





2.2 Diagnostic Question 05 Discussion

Cymbal Bank needs to connect its employee MongoDB database to a new human resources web application on the same network. Both the database and the application are autoscaled with the help of Instance templates. As the Security Administrator and Project Editor, you have been tasked with allowing the application to read port 27017 on the database.

What should you do?

A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

B. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow ICMP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

C. Create a user account for the database admin and a service account for the application. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-admin-user-account

D. Create user accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--deny UDP:27017
--source-service-accounts web-application-user-account
--target-service-accounts database-admin-user-account

2.2 Diagnostic Question 05 Discussion

Cymbal Bank needs to connect its employee MongoDB database to a new human resources web application on the same network. Both the database and the application are autoscaled with the help of Instance templates. As the Security Administrator and Project Editor, you have been tasked with allowing the application to read port 27017 on the database.

What should you do?

A. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

B. Create service accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow ICMP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-service-account

C. Create a user account for the database admin and a service account for the application. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--allow TCP:27017
--source-service-accounts web-application-service-account
--target-service-accounts database-admin-user-account

D. Create user accounts for the application and database. Create a firewall rule using:
gcloud compute firewall-rules create ALLOW_MONGO_DB
--network network-name
--deny UDP:27017
--source-service-accounts web-application-user-account
--target-service-accounts database-admin-user-account

2.4 Diagnostic Question 07 Discussion

You are configuring firewall rules for securing a set of microservices (MS1, MS2, MS3) running in separate managed instance groups (MIGs) of VMs in a single subnet of a VPC network. The primary range of the VPC network is 10.128.128.0/20. MS1 will send requests to MS2 on TCP port 8443; MS2 will send requests to MS3 on TCP port 8663; and MS3 will send requests to MS1 on TCP port 8883. There will be no other communication to or between these microservices.

Select a simple and secure firewall configuration to support this traffic requirement.

A. Create service accounts (S1, S2, S3) for the microservices, and assign those service accounts to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source S1 to target S2; for TCP 8663 from source S2 to target S3, and for TCP 8883 from source S3 to target S1.

B. Create network tags (T1, T2. T3) for the microservices, and assign those network tags to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source T1 to target T2; for TCP 8663 from source T2 to target T3; and for TCP 8883 from source T3 to target T4.

C. Create service accounts (S1, S2, S3) for the microservices, and assign those service accounts to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source 10.128.128.0/20 to target S2; for TCP 8663 from source 10.128.128.0/20 to target S3; for TCP and 8883 from source 10.128.128.0/20 to target S1.

D. Create network tags (T1, T2, T3) for the microservices, and assign those network tags to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source 10.128.128.0/20 to target T2; for TCP 8663 from source 10.128.128.0/20 to target T3; and for TCP 8883 from source 10.128.128.0/20 to target T1.

2.4 Diagnostic Question 07 Discussion

You are configuring firewall rules for securing a set of microservices (MS1, MS2, MS3) running in separate managed instance groups (MIGs) of VMs in a single subnet of a VPC network. The primary range of the VPC network is 10.128.128.0/20. MS1 will send requests to MS2 on TCP port 8443; MS2 will send requests to MS3 on TCP port 8663; and MS3 will send requests to MS1 on TCP port 8883. There will be no other communication to or between these microservices.

Select a simple and secure firewall configuration to support this traffic requirement.

A. **Create service accounts (S1, S2, S3) for the microservices, and assign those service accounts to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source S1 to target S2; for TCP 8663 from source S2 to target S3, and for TCP 8883 from source S3 to target S1.**

B. Create network tags (T1, T2. T3) for the microservices, and assign those network tags to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source T1 to target T2; for TCP 8663 from source T2 to target T3; and for TCP 8883 from source T3 to target T4.

C. Create service accounts (S1, S2, S3) for the microservices, and assign those service accounts to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source 10.128.128.0/20 to target S2; for TCP 8663 from source 10.128.128.0/20 to target S3; for TCP and 8883 from source 10.128.128.0/20 to target S1.

D. Create network tags (T1, T2, T3) for the microservices, and assign those network tags to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source 10.128.128.0/20 to target T2; for TCP 8663 from source 10.128.128.0/20 to target T3; and for TCP 8883 from source 10.128.128.0/20 to target T1.

5.2 Diagnostic Question 06 Discussion

Cymbal Bank has set up firewall rules for a VPC. You want to monitor them to determine which Deny rules are triggering to block traffic over the next 24 hours.

Select the simplest setup and process to accomplish this.

A. Enable the Firewall Insights API. Enable the Firewall Rules logging for all rules. Configure an observation period starting immediately and lasting 24h. After 24h have passed, view the Firewall Insights Deny rules with hits page.

B. Enable the Firewall Insights API. Configure an observation period starting immediately and lasting 24h. After 24h have passed, view the Firewall Insights Deny rules with hits page.

C. Enable the Firewall Insights API. After 24h have passed, view the Firewall Insights Deny rules with hits page.

D. Enable Firewall Rules logging for all rules. Configure an observation period starting immediately and lasting 24h. After 24h have passed, view the Firewall Insights Deny rules with hits page.

5.2 Diagnostic Question 06 Discussion

Cymbal Bank has set up firewall rules for a VPC. You want to monitor them to determine which Deny rules are triggering to block traffic over the next 24 hours.

Select the simplest setup and process to accomplish this.

A. **Enable the Firewall Insights API. Enable the Firewall Rules logging for all rules. Configure an observation period starting immediately and lasting 24h. After 24h have passed, view the Firewall Insights Deny rules with hits page.**

B. Enable the Firewall Insights API. Configure an observation period starting immediately and lasting 24h. After 24h have passed, view the Firewall Insights Deny rules with hits page.

C. Enable the Firewall Insights API. After 24h have passed, view the Firewall Insights Deny rules with hits page.

D. Enable Firewall Rules logging for all rules. Configure an observation period starting immediately and lasting 24h. After 24h have passed, view the Firewall Insights Deny rules with hits page.

2.4 Diagnostic Question 08 Discussion

You are trying to determine which firewall rules are incorrectly blocking requests between two VMs running within a VPC network: VM1 and VM2. Firewall logging is enabled for all firewall rules, including metadata. The Firewall Insights and Recommendations API are also enabled. All insights are enabled, and an observation period is set over a period capturing the blocked requests.

Select a valid troubleshooting approach to find the incorrectly configured firewall rule.

A. On the Firewall Insights page of the Google Cloud Console, find the names of the deny firewall rules with hits to identify rules that are blocking requests. On the Legacy Logs Viewer or Logs Explorer page, view the firewall logs and filter for logs that match those rules by name, using jsonPayload.rule_details.reference field, matching the names of the deny firewall rules with hits.

B. On the Logs Explorer or Legacy Logs Viewer page, view the firewall logs, and filter for logs that match the source and destination VMs VM1 and VM2, using the jsonPayload.instance.project_id, jsonPayload.instance.vm_name, jsonPayload.instance.region, and jsonPayload.instance.zone, jsonPayload.remote_instance.vm_name, jsonPayload.remote_instance.region, and jsonPayload.remote_instance.zone.

C. On the Logs Explorer or Legacy Logs Viewer page, view the firewall logs, and filter for logs that match the destination VM2 in the VPC, using the jsonPayload.instance.project_id, jsonPayload.instance.vm_name, jsonPayload.instance.region, and jsonPayload.instance.zone fields.

D. On the Firewall Insights landing page of the Google Cloud Console, find the names of the allow firewall rules with no hits to identify rules that are not allowing requests. On the Logs Viewer or Explorer page, view the firewall logs and filter for logs matching those rules by name, using jsonPayload.rule_details.reference field (matching the names of the allow firewall rules with no hits).

2.4 Diagnostic Question 08 Discussion

You are trying to determine which firewall rules are incorrectly blocking requests between two VMs running within a VPC network: VM1 and VM2. Firewall logging is enabled for all firewall rules, including metadata. The Firewall Insights and Recommendations API are also enabled. All insights are enabled, and observation period set over a period capturing the blocked requests.

Select a valid troubleshooting approach to find the incorrectly configured firewall rule.

A. On the Firewall Insights page of the Google Cloud Console, find the names of the deny firewall rules with hits to identify rules that are blocking requests. On the Legacy Logs Viewer or Logs Explorer page, view the firewall logs and filter for logs that match those rules by name, using jsonPayload.rule_details.reference field, matching the names of the deny firewall rules with hits.

B. On the Logs Explorer or Legacy Logs Viewer page, view the firewall logs, and filter for logs that match the source and destination VMs VM1 and VM2, using the jsonPayload.instance.project_id, jsonPayload.instance.vm_name, jsonPayload.instance.region, and jsonPayload.instance.zone, jsonPayload.remote_instance.vm_name, jsonPayload.remote_instance.region, and jsonPayload.remote_instance.zone.

C. On the Logs Explorer or Legacy Logs Viewer page, view the firewall logs, and filter for logs that match the destination VM2 in the VPC, using the jsonPayload.instance.project_id, jsonPayload.instance.vm_name, jsonPayload.instance.region, and jsonPayload.instance.zone fields.

D. On the Firewall Insights landing page of the Google Cloud Console, find the names of the allow firewall rules with no hits to identify rules that are not allowing requests. On the Logs Viewer or Explorer page, view the firewall logs and filter for logs matching those rules by name, using jsonPayload.rule_details.reference field (matching the names of the allow firewall rules with no hits).

2.2 Diagnostic Question 06 Discussion

Cymbal Bank has designed an application to detect credit card fraud that will analyze sensitive information. The application that's running on a Compute Engine instance is hosted in a new subnet on an existing VPC. Multiple teams who have access to other VMs in the same VPC must access the VM. You want to configure the access so that unauthorized VMs or users from the internet can't access the fraud detection VM.

What should you do?

A. Use subnet isolation. Create a service account for the fraud detection VM. Create one service account for all the teams' Compute Engine instances that will access the fraud detection VM. Create a new firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <one service account for all teams>
--target-service-accounts <fraud detection engine's service account>

B. Use target filtering. Create two tags called 'app' and 'data'. Assign the 'app' tag to the Compute Engine instance hosting the Fraud Detection App (source), and assign the 'data' tag to the other Compute Engine instances (target). Create a firewall rule to allow all ingress communication on this tag.

B. Use subnet isolation. Create a service account for the fraud detection engine. Create service accounts for each of the teams' Compute Engine instances that will access the engine. Add a firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <list of service accounts>
--target-service-accounts <fraud detection engine's service account>

D. Use target filtering. Create a tag called 'app', and assign the tag to both the source and the target. Create a firewall rule to allow all ingress communication on this tag.

2.2 Diagnostic Question 06 Discussion

Cymbal Bank has designed an application to detect credit card fraud that will analyze sensitive information. The application that's running on a Compute Engine instance is hosted in a new subnet on an existing VPC. Multiple teams who have access to other VMs in the same VPC must access the VM. You want to configure the access so that unauthorized VMs or users from the internet can't access the fraud detection VM.

What should you do?

A. Use subnet isolation. Create a service account for the fraud detection VM. Create one service account for all the teams' Compute Engine instances that will access the fraud detection VM. Create a new firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <one service account for all teams>
--target-service-accounts <fraud detection engine's service account>

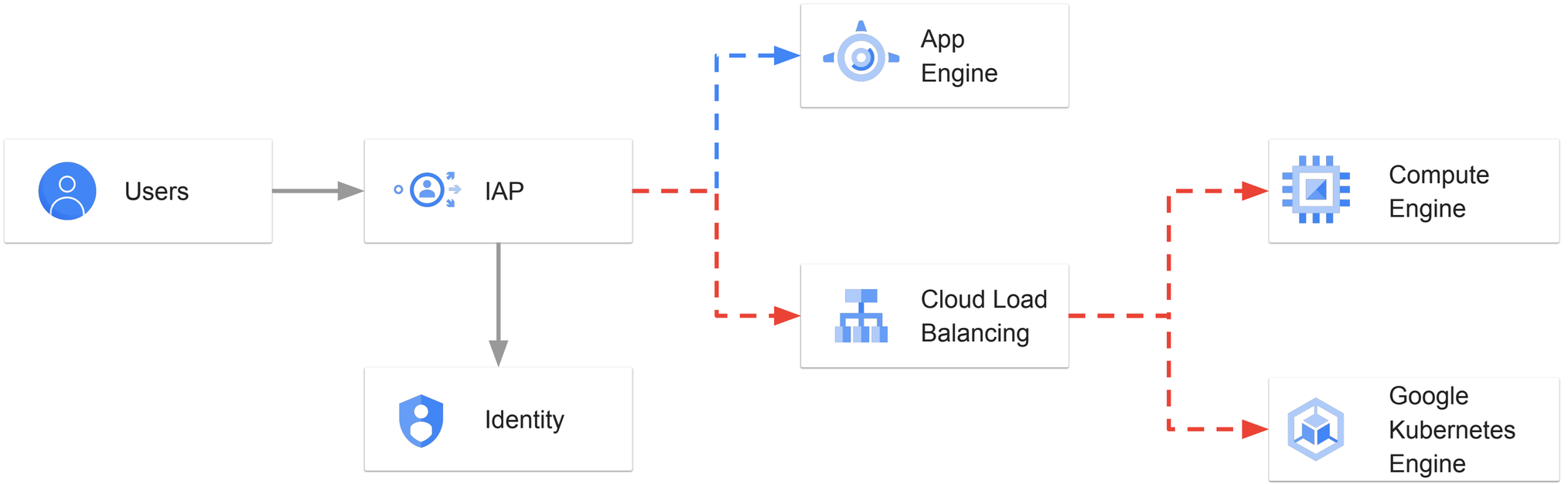
B. Use target filtering. Create two tags called 'app' and 'data'. Assign the 'app' tag to the Compute Engine instance hosting the Fraud Detection App (source), and assign the 'data' tag to the other Compute Engine instances (target). Create a firewall rule to allow all ingress communication on this tag.

B. Use subnet isolation. Create a service account for the fraud detection engine. Create service accounts for each of the teams' Compute Engine instances that will access the engine. Add a firewall rule using:
gcloud compute firewall-rules create ACCESS_FRAUD_ENGINE
--network <network name>
--allow TCP:80
--source-service-accounts <list of service accounts>
--target-service-accounts <fraud detection engine's service account>

D. Use target filtering. Create a tag called 'app', and assign the tag to both the source and the target. Create a firewall rule to allow all ingress communication on this tag.

Identity-Aware Proxy (IAP)

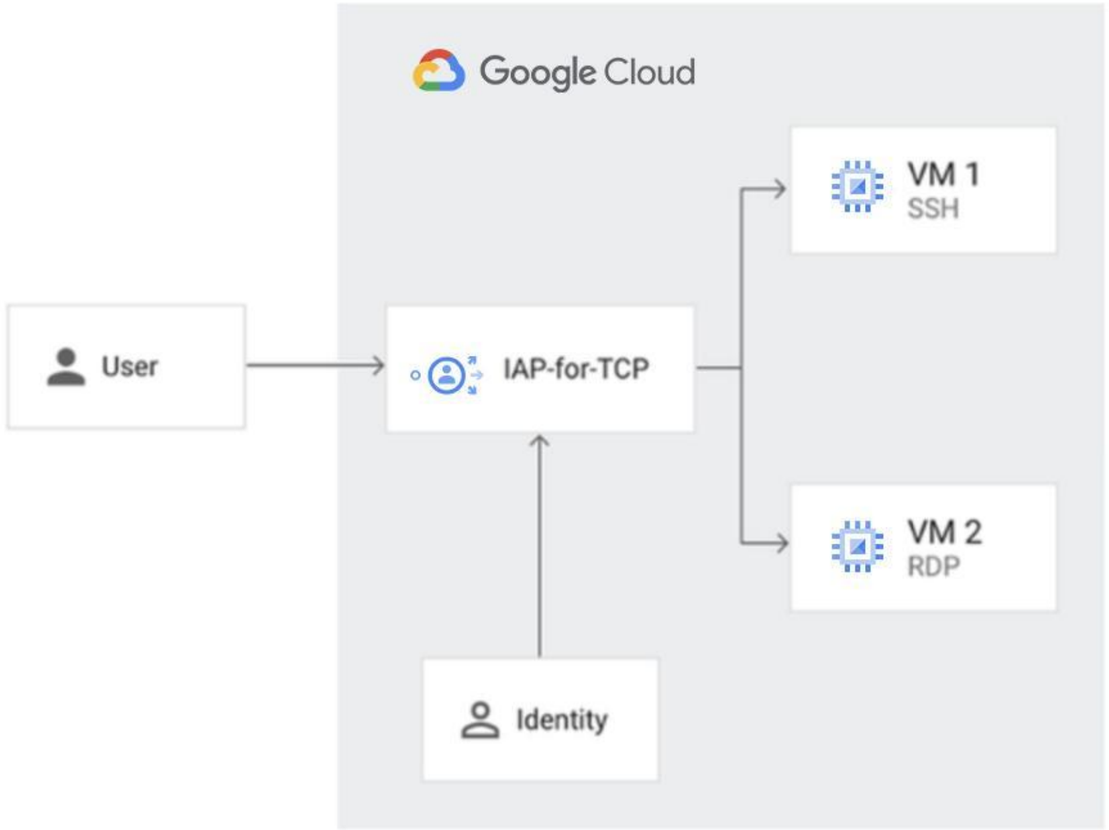
Connect through Identity-Aware Proxy



Identity-aware proxy for TCP

Common pattern

- Tunnel TCP traffic to instances without exposing them to the public internet
- Traffic between client and IAP is wrapped in HTTPS
- Access controlled by user identity and IAM



SSH

- IAP for TCP can be easily used instead of a bastion host by using Cloud SDK:

```
gcloud compute ssh user@instance --zone
<zone>
```

Exam Tip: *It's a best practise to also use IAP to enable administrative access to VMs (ssh, rdp) which do not have external IPs.*

Identity-aware proxy for web apps

Central enforcement

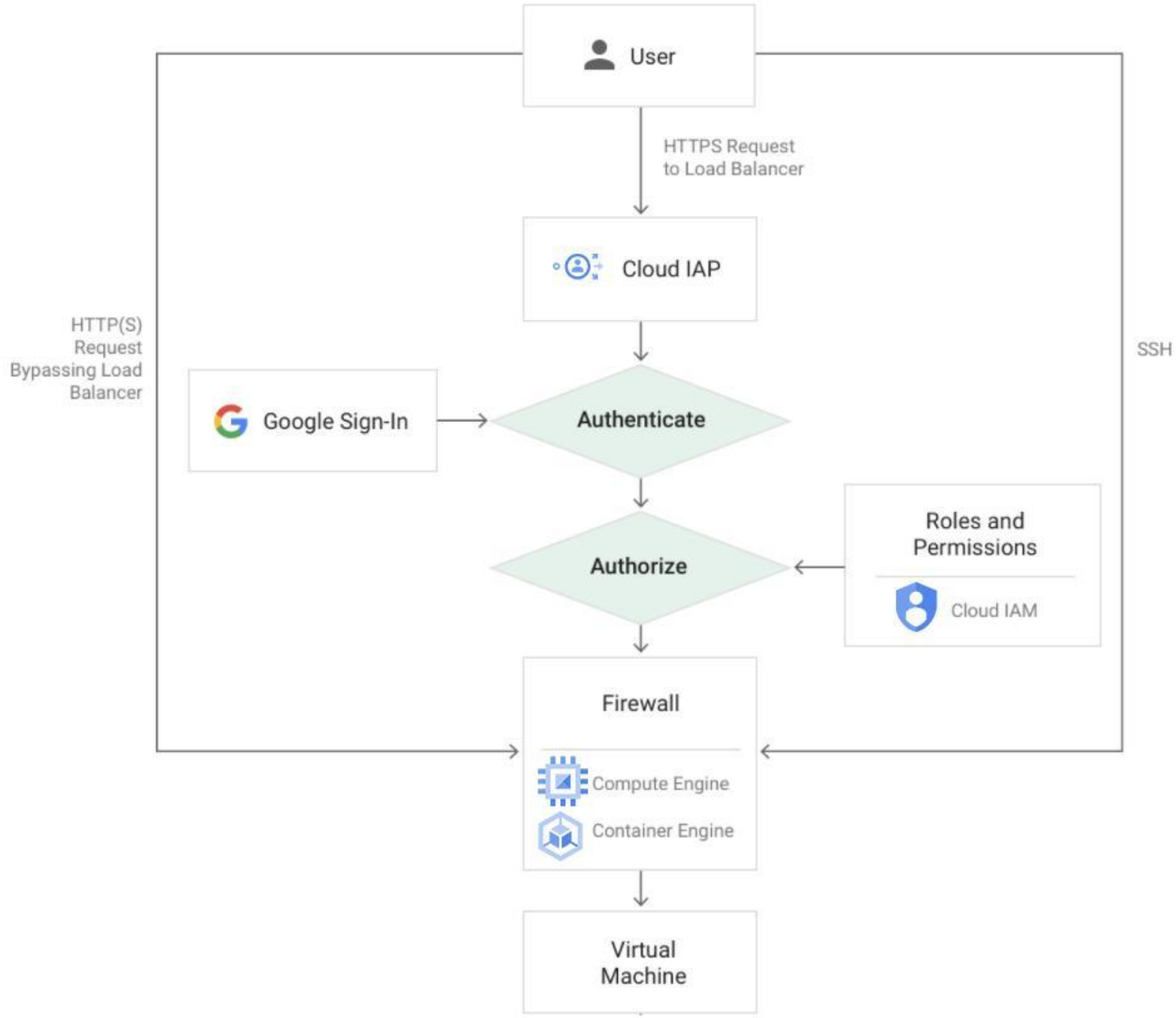
- Single point of control for managing user access
- Security team can define and enforce policy

Access control

- Control access by user identity
- Apply policy by group membership
- Supports 2FA security keys

Deployment

- Little to no change to applications
- No need to implement own authentication for each application
- Integrated with HTTP(s) load balancer



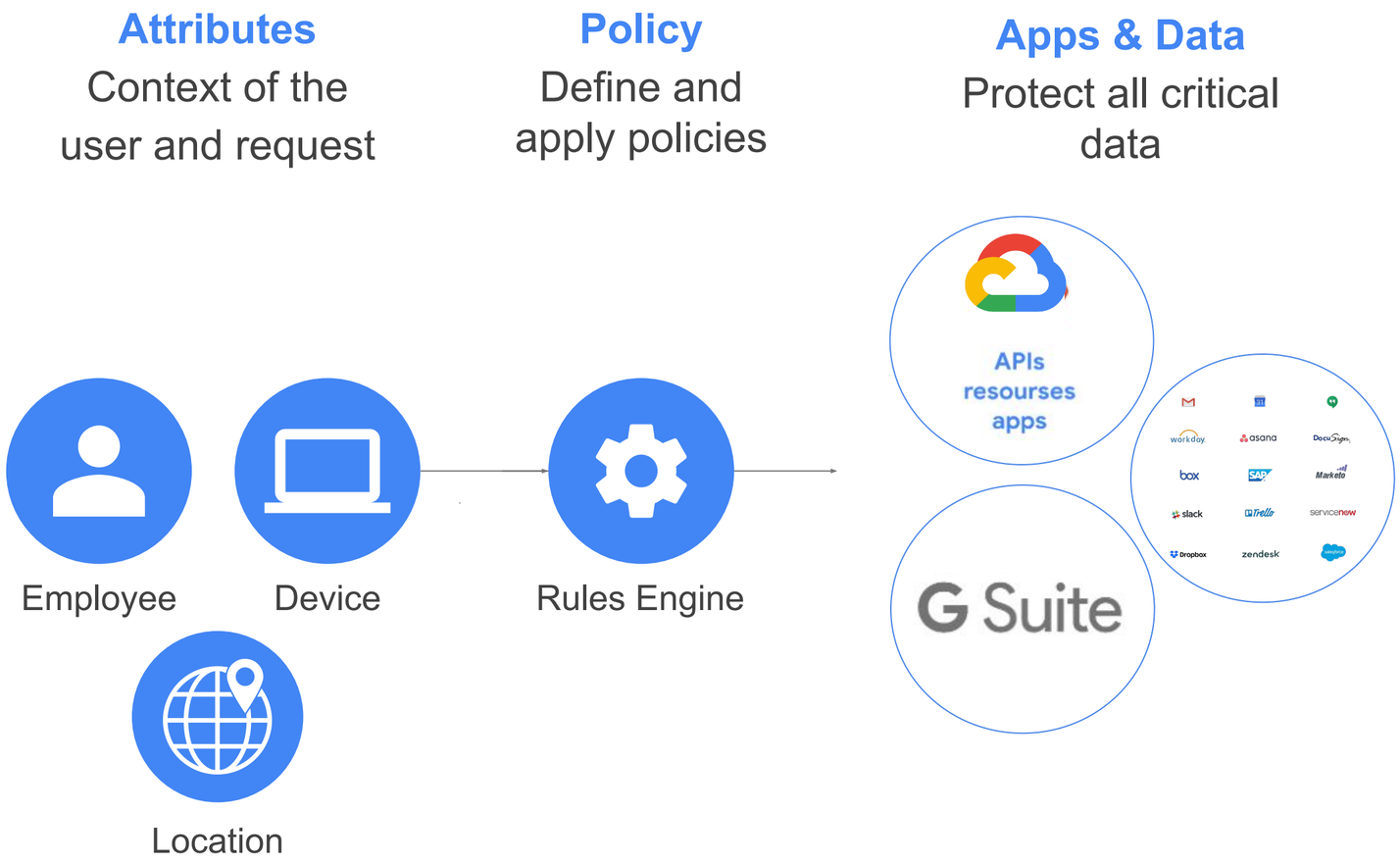
Access Context Manager - Access levels

Context-Aware Access Suite of Products collects attributes and data

- Endpoint verification collects device identity and security posture
- Cloud Identity provides user information

Access Context Manager Defines Authorization Rules

- Define rules around geography, device status, time of day, etc.for granting access



User + Device + Context is the new security perimeter

2.1 Diagnostic Question 03 Discussion

Your organization has a website running on Compute Engine. This instance only has a private IP address. You need to provide SSH access to an on-premises developer who will debug the website from the authorized on-premises location only.

How do you enable this?

A. Set up Cloud VPN. Set up an unencrypted tunnel to one of the hosts in the network. Create outbound or egress firewall rules. Use the private IP address to log in using a gcloud ssh command.

B. Use SOCKS proxy over SSH. Set up an SSH tunnel to one of the hosts in the network. Create the SOCKS proxy on the client side.

C. Use the default VPC's firewall. Open port 22 for TCP protocol using the Google Cloud Console.

D. Use Identity-Aware Proxy (IAP). Set up IAP TCP forwarding by creating ingress firewall rules on port 22 for TCP using the gcloud command.

2.1 Diagnostic Question 03 Discussion

Your organization has a website running on Compute Engine. This instance only has a private IP address. You need to provide SSH access to an on-premises developer who will debug the website from the authorized on-premises location only.

How do you enable this?

A. Set up Cloud VPN. Set up an unencrypted tunnel to one of the hosts in the network. Create outbound or egress firewall rules. Use the private IP address to log in using a gcloud ssh command.

B. Use SOCKS proxy over SSH. Set up an SSH tunnel to one of the hosts in the network. Create the SOCKS proxy on the client side.

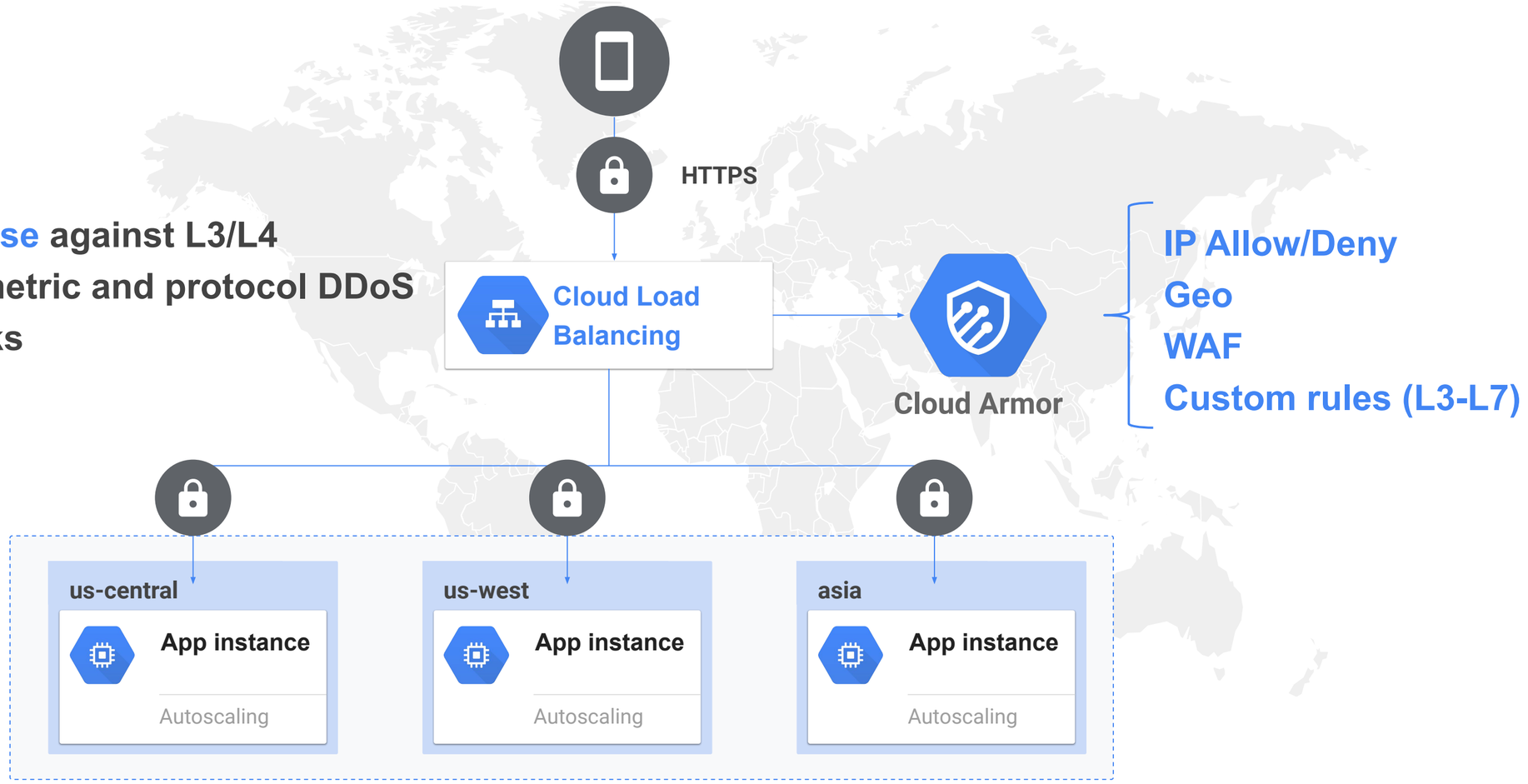
C. Use the default VPC's firewall. Open port 22 for TCP protocol using the Google Cloud Console.

D. Use Identity-Aware Proxy (IAP). Set up IAP TCP forwarding by creating ingress firewall rules on port 22 for TCP using the gcloud command.

Cloud Armor

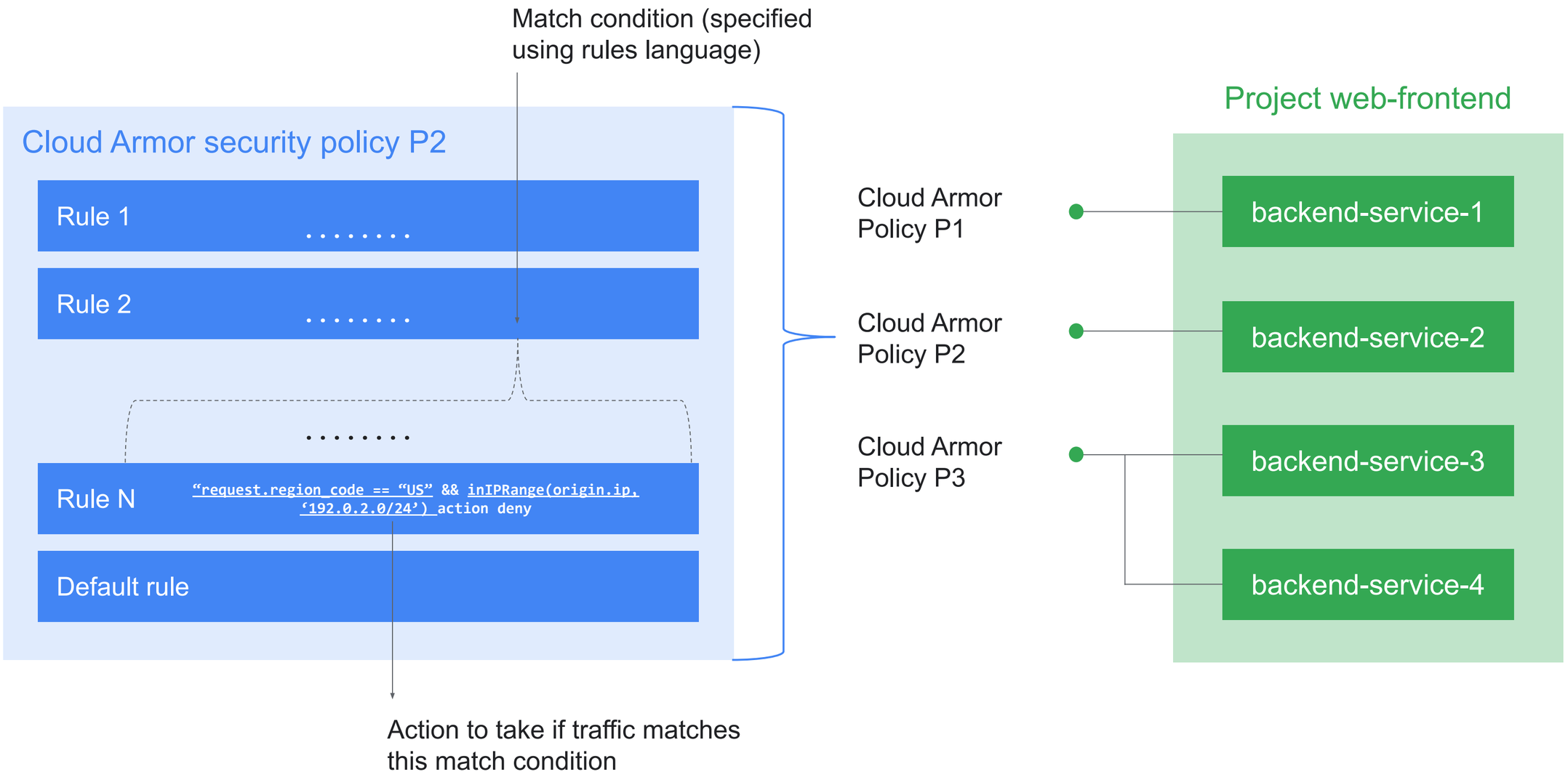
Cloud Armor: DDoS Protection & WAF

Defense against L3/L4 volumetric and protocol DDoS attacks



Google Cloud

Google Cloud Armor Security Policies



What’s in a Cloud Armor rule?

Rules language: Based on

Common Expressions Language (CEL)

[https://github.com/google/cel-spec]

Match Condition

Specifies the matching criteria to be evaluated on the incoming request before enforcing the corresponding action. Can be basic (IP allow/deny) or complex (CEL expression) across L3-L7 attributes

Action

Action to take when incoming traffic satisfies match condition

Priority

Rules are evaluated in priority order in a policy (lowest -> highest)

Preview

Put rule in Preview mode to log its behavior without actually taking the action

Configure policy

Name *
cloud-armor-policy
Lowercase letters, numbers, hyphens allowed

Description

Policy type

- (•) Backend security policy
- ( ) Edge security policy

Default rule action

- ( ) Allow
- (•) Deny

Deny status
403 (Forbidden)

NEXT STEP

Apply policy to targets (optional)

Targets are Google Cloud Platform resources that you want to control access to.
You can only use non-CDN HTTP(S) load balancer backend services as targets.

Type 1
Load balancer backend ser...

Backend Service target 1 *

Filter Type to filter

web-backend
Load balancer: web-lb

+ ADD TARGET

You can also add/edit targets after the p

NEXT STEP

RULES | TARGETS | LOGS

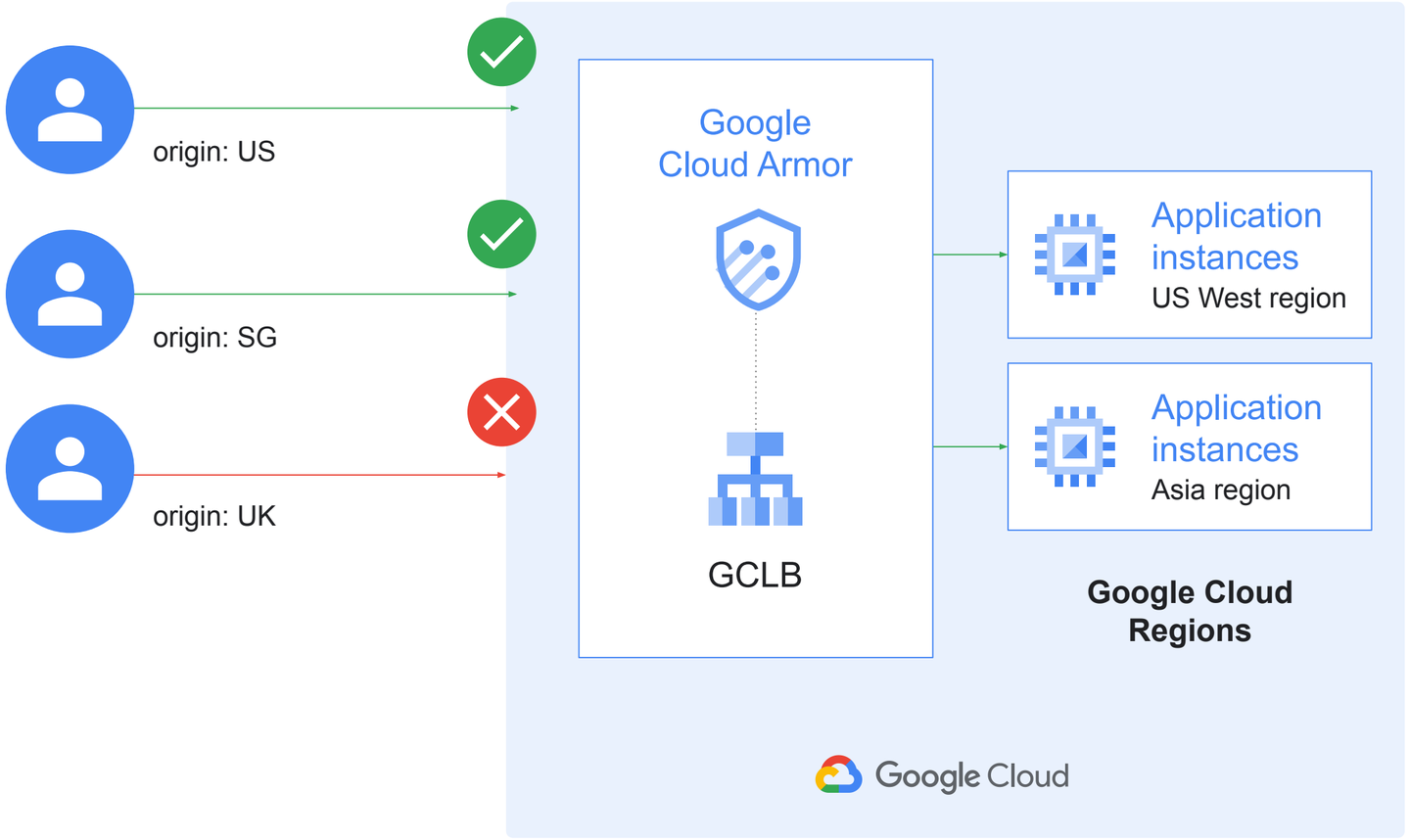
Rules are evaluated by priority: Lower numbers are evaluated first. Learn more

ADD RULE | DELETE | MORE

Filter Enter property name or value

Action	Type	Match	Description	Priority
Deny (403)	IP addresses/ranges	* (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647

Geography & ASN Based Access Controls



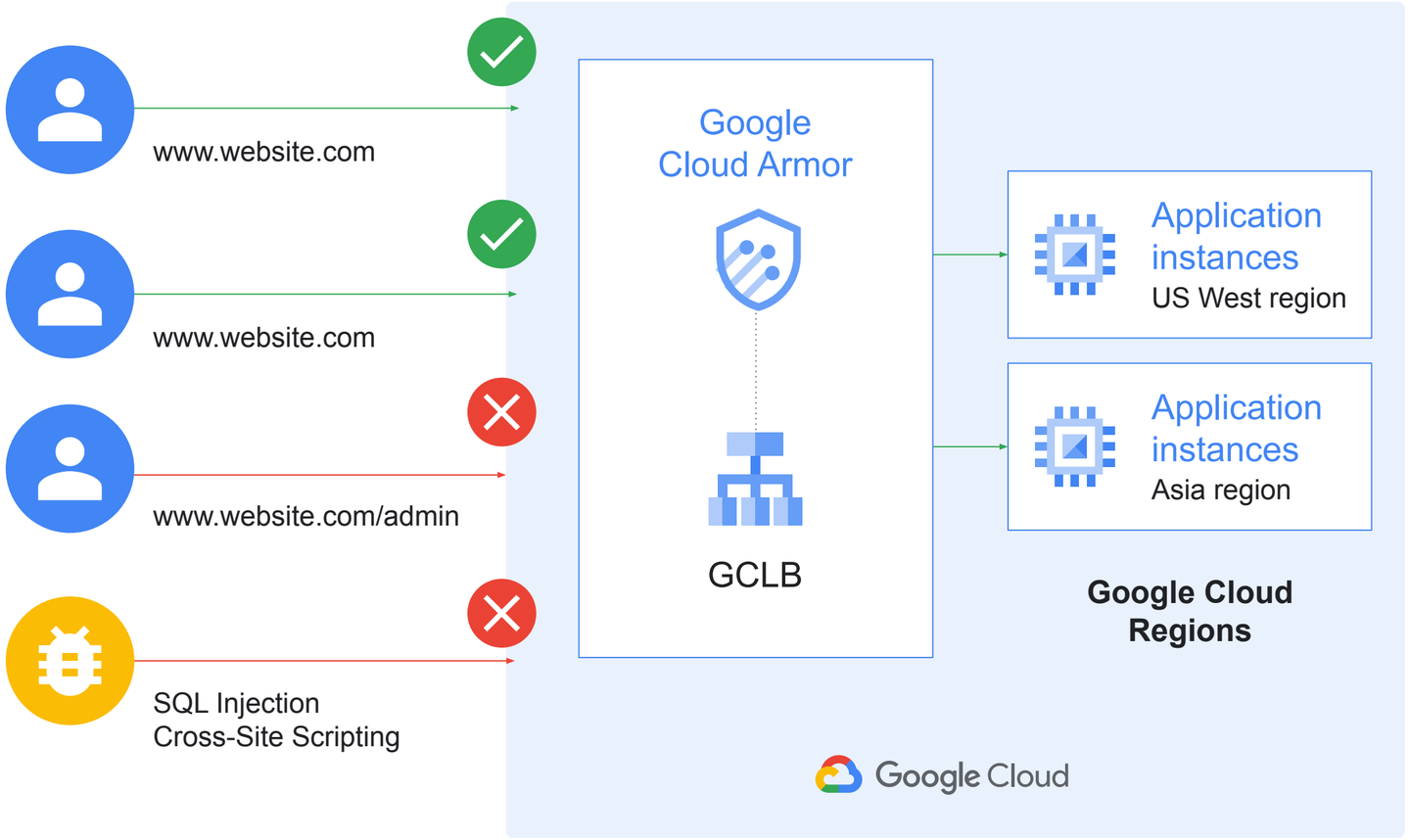
app2-protection

Description (Optional): **Geobased Acess Control Policy**

The policy contains: 3 rules

Match	Action	Description	Priority
request.origin == 'US'	Allow	allow US	10
request.origin == 'SG'	Allow	allow Singapore	20
* (All IP addresses)	Deny (403)	Default rule, higher priority overrides it	2,147,483,647

Layer 7 Traffic Filtering & WAF



prod-high

Description: protect high security applications

Contains	Applies to
4 rules	1 target

Rules | Targets | Logs

Rules are evaluated by priority: Lower numbers are evaluated first. Learn more

Search by matches, action or priority | Columns

Add rule | Delete | More

Action	Type	Match	Description	Priority
Deny (403)		request.path.contains("/admin")	block external access to admin portal	100
Deny (403)		evaluatePreconfiguredExpr('xss-stable')	block XSS	200
Deny (403)		evaluatePreconfiguredExpr('sqli-stable')	block SQLi	210
Allow	IP addresses/ranges	* (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647

Cloud Armor

#GCPSketchnote

@PVERGADIA THECLOUDGIRL.DEV

10.29.2020

ERIN: User traffic on our internet facing service is growing rapidly!

We need a solution to get protection from DDoS & Web attacks.

SAM: And so are the malicious attacks!

Cloud Armor!

What is Cloud Armor?

Defend against application layer attacks (SQLi, XSS, etc). Use in combination with IAP.

Mitigate infrastructure DDoS attacks with Global HTTP(s) Load Balancing (TCP SYN floods, Amplification attacks, IP fragmentation attacks, etc.

Telemetry: Decisions sent to Cloud logging, monitoring and Security command center.

Allow or block traffic based on IP, Geo, and custom match parameters (L3-L7, etc).

How do security policies apply?

Match condition (specified using rules language)

CLOUD ARMOR security policy P2

- Rule 1 ……
- Rule 2 ……
- ……
- Rule N `"request. region_code == "US" && inIPRange (origin.ip,"192.0.2.0/24")` action deny
- Default rule

Action to take if traffic matches this match condition

CLOUD ARMOR: SECURITY POLICIES

PROJECT web-frontend

- CLOUD ARMOR Policy P1 → backend-service-1
- CLOUD ARMOR Policy P2 → backend-service-2
- CLOUD ARMOR Policy P3 → backend-service-3, backend-service-4

How does Cloud Armor work?

CLOUD ARMOR: DDOS PROTECTION & WAF

Defense against L3/L4 volumetric and protocol DDoS attacks

HTTPs

Cloud CDN

HTTP(s) Load Balancing

- IP Allow/Deny
- Geo
- WAF
- Custom rules (L3-L7)

Internet

Cloud Provider / Customer Datacenter: External Application

GKE Cluster

Autoscaling: App Instance

Hybrid or Multi Cloud Workload

L3/L4 Volumetric DDoS Protection

- DNS Amplification
- SYN Flood
- ICMP Flood
- Slowloris

Geography Based Access Controls

- origin: US
- origin: UK
- origin: SG

Layer 7 Traffic Filtering & WAF

- www.website.com
- www.website.com
- website.com/admin
- SQL Injection
- Cross-Site Scripting

Google Cloud

Cloud Armor

Cloud Load Balancing

Application/ Service

What do I get in visibility & telemetry?

Cloud Security Command Center

Finding & Assets

Pre request logging

Cloud Armor

Real time telemetry

Cloud Logging

Cloud Monitoring

3.2 Diagnostic Question 03 Discussion

Cymbal Bank wants to protect their services, which are deployed behind an HTTP(S) load balancer, from L7 distributed denial of service (DDoS), SQL injection (SQLi), and cross-site scripting (XSS) attacks.

A. Configure Google Cloud Armor with the appropriate rules.
B. Configure a VM with appropriate scanning and filtering software in front of the HTTP(S) load balancer.
C. Configure Google Cloud WAF with the appropriate rules.
D. Configure Cloud NAT with the appropriate rules.

Select the simplest approach to accomplish this.

3.2 Diagnostic Question 03 Discussion

Cymbal Bank wants to protect their services, which are deployed behind an HTTP(S) load balancer, from L7 distributed denial of service (DDoS), SQL injection (SQLi), and cross-site scripting (XSS) attacks.

A. **Configure Google Cloud Armor with the appropriate rules.**
B. Configure a VM with appropriate scanning and filtering software in front of the HTTP(S) load balancer.
C. Configure Google Cloud WAF with the appropriate rules.
D. Configure Cloud NAT with the appropriate rules.

Select the simplest approach to accomplish this.

2.1 Diagnostic Question 01 Discussion

Cymbal Bank has published an API that internal teams will use through the HTTPS load balancer. You need to limit the API usage to 200 calls every hour. Any exceeding usage should inform the users that servers are busy.

Which gcloud command would you run to throttle the load balancing for the given specification?

A. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-429
--enforce-on-key=HTTP-HEADER

B. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=60
--conform-action=deny
--exceed-action=deny-404
--enforce-on-key=HTTP-HEADER

C. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=deny
--exceed-action=deny-403
--enforce-on-key=HTTP-HEADER

D. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges="<source range>"
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-500
--enforce-on-key=IP

2.1 Diagnostic Question 01 Discussion

Cymbal Bank has published an API that internal teams will use through the HTTPS load balancer. You need to limit the API usage to 200 calls every hour. Any exceeding usage should inform the users that servers are busy.

Which gcloud command would you run to throttle the load balancing for the given specification?

A. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-429
--enforce-on-key=HTTP-HEADER

B. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=throttle
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=60
--conform-action=deny
--exceed-action=deny-404
--enforce-on-key=HTTP-HEADER

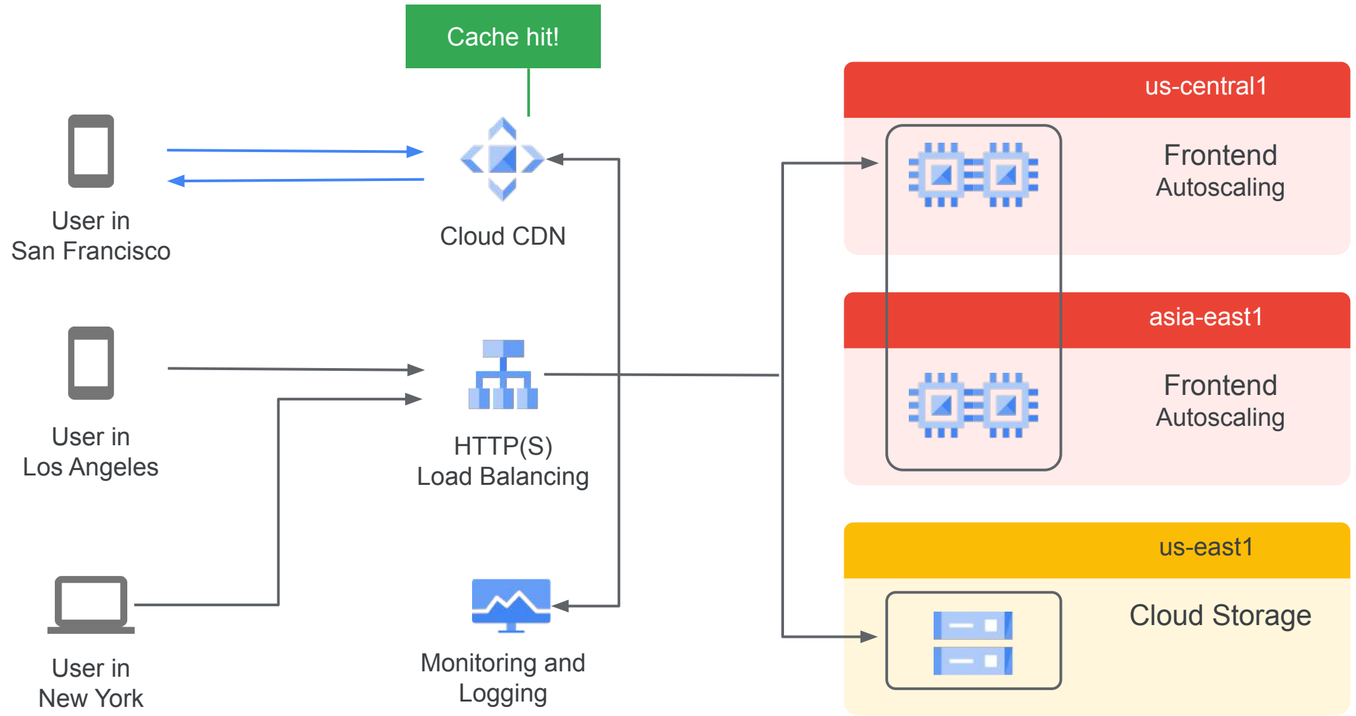
C. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges=source-range
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=deny
--exceed-action=deny-403
--enforce-on-key=HTTP-HEADER

D. gcloud compute security-policies rules create priority
--security-policy sec-policy
--src-ip-ranges="<source range>"
--action=rate-based-ban
--rate-limit-threshold-count=200
--rate-limit-threshold-interval-sec=3600
--conform-action=allow
--exceed-action=deny-500
--enforce-on-key=IP

Cloud CDN

Cloud CDN

- Cache static resources at Google Cloud edge locations.
- Easily integrate with an HTTP(S) load balancer.
- Configure cache keys and TTL and optional cache invalidation.
- Cache on-premises or other external origins.
- Use signed URLs and cookies for authorized anonymous access.



Cloud CDN

- **CDN Cache modes** control the factors that determine whether on not Cloud CDN caches your content. Three Cache modes:
  - `CACHE_ALL_STATIC`
  - `USE_ORIGIN_HEADERS`
  - `FORCE_CACHE_ALL`

- **Cache-control headers** used to determine what should be cached and for how long
  - To be set for web servers at app level: cache-control: public, max-age=XXX

- **How to invalidate cached content** to remove an object from the cache prior to its normal expiration time. You can force an object or set of objects to be ignored by the cache by requesting a cache invalidation.

Cloud CDN

#GCPSketchnote

@PVERGADIA THECLOUDGIRL.DEV

9.21.2020

Our website is slow, cost is high and users are frustrated!!

It's because our users are across the globe and servers are only in the US.

We need a tool that helps

Reduce Latency | Reduce Cost | Reduce Load

SYS ADMIN SAM

DEVELOPER ERIN

Cloud CDN!

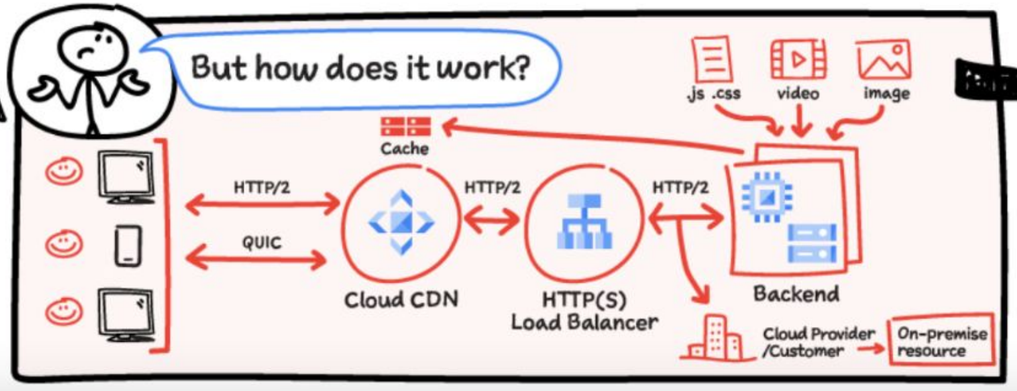
What is Cloud CDN?

CONTENT DELIVERY NETWORK
= ACCELERATE WEB & VIDEO CONTENT

.js .css | video | image

Origin Server | Google Edge Server | User

But how does it work?



How do I use Cloud CDN?

1. Enable CDN
2. Select Cache Modes
   - Cache all content
   - Use origin header Cache-control
   - Force cache all content
3. Set TTL (Time to live)

How does Cloud CDN look for files in cache?

CACHE KEY = Protocol + https://example.com/images/cat.jpg?user=a

Host | Query string

How is Anycast IP helpful?

SINGLE IP
GLOBAL REACH

Intelligent Anycast

DNS

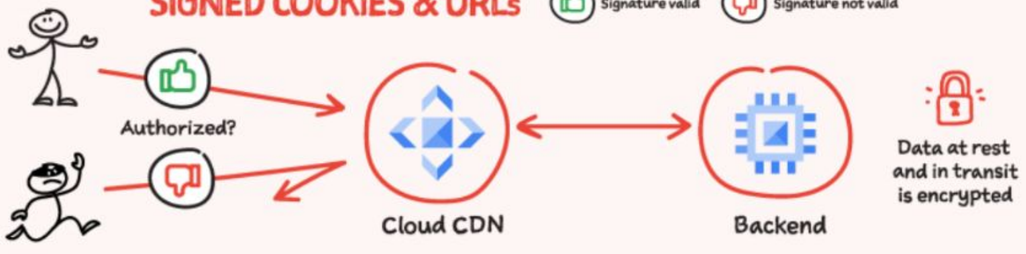
www.myapp.com
A record 120.1.1.1

How do I secure content using Cloud CDN?

SECURITY

SIGNED COOKIES & URLs

Signature valid | Signature not valid



GOOGLE MANAGED CERTIFICATE

1.1 Diagnostic Question 03 Discussion

You are a network engineer designing a solution for hosting a Cymbal Bank web application in Google Cloud. The application will serve a collection of static and dynamic web resources served over HTTPS to users worldwide. You need to design a solution that maximizes availability while minimizing average user latency.

Which of the following features of Google Cloud networking can you utilize? (Select 2)

A. Cloud CDN could be used to cache static content resources at edge locations close to end-users, increasing their availability and minimizing their latency.

B. Cloud NAT could be used to provide outbound connectivity to the internet for resources with only internal IP addresses, thereby increasing their availability.

C. Cloud Armor could be used to provide protection against DDoS and injection attacks and thereby minimize solution latency.

D. An HTTPS load balancer with a backend service connected to a set of regional MIGs, distributed over the regions closest to the users, to improve availability and minimize latency.

E. Network Intelligence Center could be used to provide network insights, enabling the web application to be deployed in a configuration with maximum availability and minimal latency.

1.1 Diagnostic Question 03 Discussion

You are a network engineer designing a solution for hosting a Cymbal Bank web application in Google Cloud. The application will serve a collection of static and dynamic web resources served over HTTPS to users worldwide. You need to design a solution that maximizes availability while minimizing average user latency.

Which of the following features of Google Cloud networking can you utilize? (Select 2)

A. **Cloud CDN could be used to cache static content resources at edge locations close to end-users, increasing their availability and minimizing their latency.**

B. Cloud NAT could be used to provide outbound connectivity to the internet for resources with only internal IP addresses, thereby increasing their availability.

C. Cloud Armor could be used to provide protection against DDoS and injection attacks and thereby minimize solution latency.

D. **An HTTPS load balancer with a backend service connected to a set of regional MIGs, distributed over the regions closest to the users, to improve availability and minimize latency.**

E. Network Intelligence Center could be used to provide network insights, enabling the web application to be deployed in a configuration with maximum availability and minimal latency.

3.3 Diagnostic Question 04 Discussion

Cymbal Bank uses Cloud CDN to cache a web application served from a backend bucket connected to a Cloud Storage bucket. You need to cache all the web-app files with appropriate time to live (TTL) except for the index.html file. The index.html file contains links to versioned files and should always be fetched or re-validated from the origin.

Select the configuration option to satisfy these requirements with minimal effort.

A. Set the Cloud CDN cache mode for the backend bucket to CACHE_ALL_STATIC.

B. Set the Cloud CDN cache mode for the backend bucket to FORCE_CACHE_ALL, and ensure that the Cache-Control metadata for index.html is set to private.

C. Set the Cloud CDN cache mode for the backend bucket to CACHE_ALL_STATIC, and ensure that the Cache-Control metadata for index.html is not set or is set to no-store, no-cache, or private.

D. Set the Cloud CDN cache mode to USE_ORIGIN_HEADERS, set the Cache-Control metadata for index.html to no-store, and set the Cache-Control headers for all the other files with appropriate TTL values.

3.3 Diagnostic Question 04 Discussion

Cymbal Bank uses Cloud CDN to cache a web application served from a backend bucket connected to a Cloud Storage bucket. You need to cache all the web-app files with appropriate time to live (TTL) except for the index.html file. The index.html file contains links to versioned files and should always be fetched or re-validated from the origin.

Select the configuration option to satisfy these requirements with minimal effort.

A. Set the Cloud CDN cache mode for the backend bucket to CACHE_ALL_STATIC.

B. Set the Cloud CDN cache mode for the backend bucket to FORCE_CACHE_ALL, and ensure that the Cache-Control metadata for index.html is set to private.

C. Set the Cloud CDN cache mode for the backend bucket to CACHE_ALL_STATIC, and ensure that the Cache-Control metadata for index.html is not set or is set to no-store, no-cache, or private.

D. Set the Cloud CDN cache mode to USE_ORIGIN_HEADERS, set the Cache-Control metadata for index.html to no-store, and set the Cache-Control headers for all the other files with appropriate TTL values.

3.3 Diagnostic Question 05 Discussion

Cymbal Bank is serving files from a backend bucket and wants to ensure time-limited read access without authentication. The backend bucket uses signed URLs to access those files. The files are also being cached in Cloud CDN. There is a problem with one of the files, and you want to delete it. You also want to immediately ensure no read access via the signed URL to the cached file copy in Cloud CDN, although the expiry time is currently set to sometime in the future.

Select the option that accomplishes this with lowest cost and effort.

A. Perform cache invalidation for the file using the full path.

B. Perform cache invalidation for the file using the path and excluding the query parameters used for the signed URL.

C. Update the expiry time for the signed URL to be the current time.

D. Delete the key used to create the signed URL.

3.3 Diagnostic Question 05 Discussion

Cymbal Bank is serving files from a backend bucket and wants to ensure time-limited read access without authentication. The backend bucket uses signed URLs to access those files. The files are also being cached in Cloud CDN. There is a problem with one of the files, and you want to delete it. You also want to immediately ensure no read access via the signed URL to the cached file copy in Cloud CDN, although the expiry time is currently set to sometime in the future.

Select the option that accomplishes this with lowest cost and effort.

A. Perform cache invalidation for the file using the full path.

B. Perform cache invalidation for the file using the path and excluding the query parameters used for the signed URL.

C. Update the expiry time for the signed URL to be the current time.

D. Delete the key used to create the signed URL.

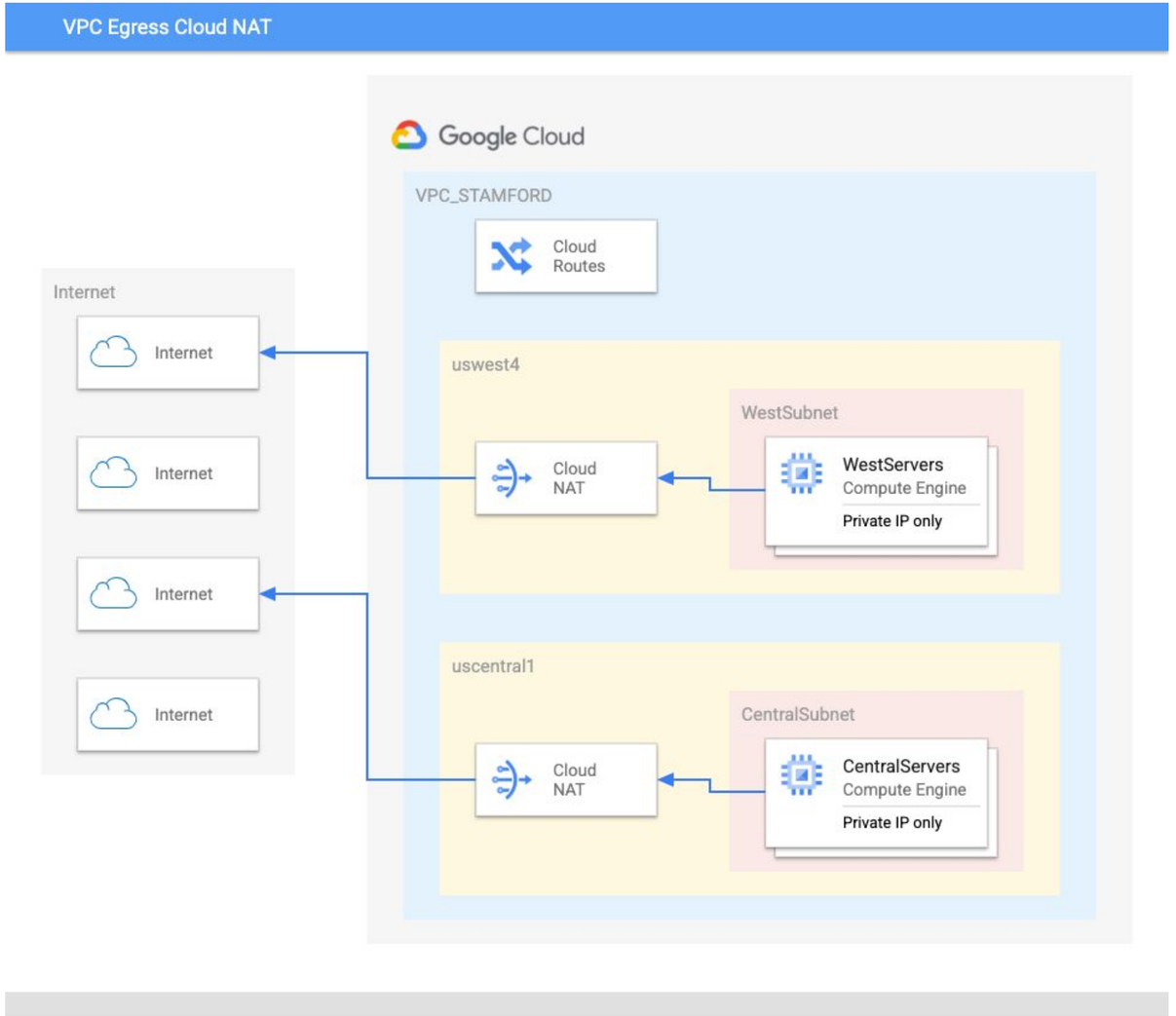
Cloud NAT

Cloud NAT

Managed (Source) NAT solution for Internet Egress.

Improved security, only outbound connections to the Internet for those resources using “Default Internet Gateway”

- Always a Regional resource
- Works for subnet primary and secondary IP ranges
- Manual vs Automatic IPs
  - Manual = Static IPs
    - Uses a configured set of public IPs to use as source addresses
    - More consistent
    - Under allocation of IPs can result in drops
  - Automatic = Dynamic IPs (Recommended when port exhaustion might be a concern)
    - Auto adds or removes source addresses based on usage
    - More Scalable
    - GCP auto-assigned addresses



Cloud NAT Advanced Settings

Port Allocation

- The number of NAT source IP address and source port tuples that a Cloud NAT gateway reserves for a VM.
- Each Cloud NAT IP can support 64,512 source ports and divide them between VMs.

Standard Port Allocation (defaut)

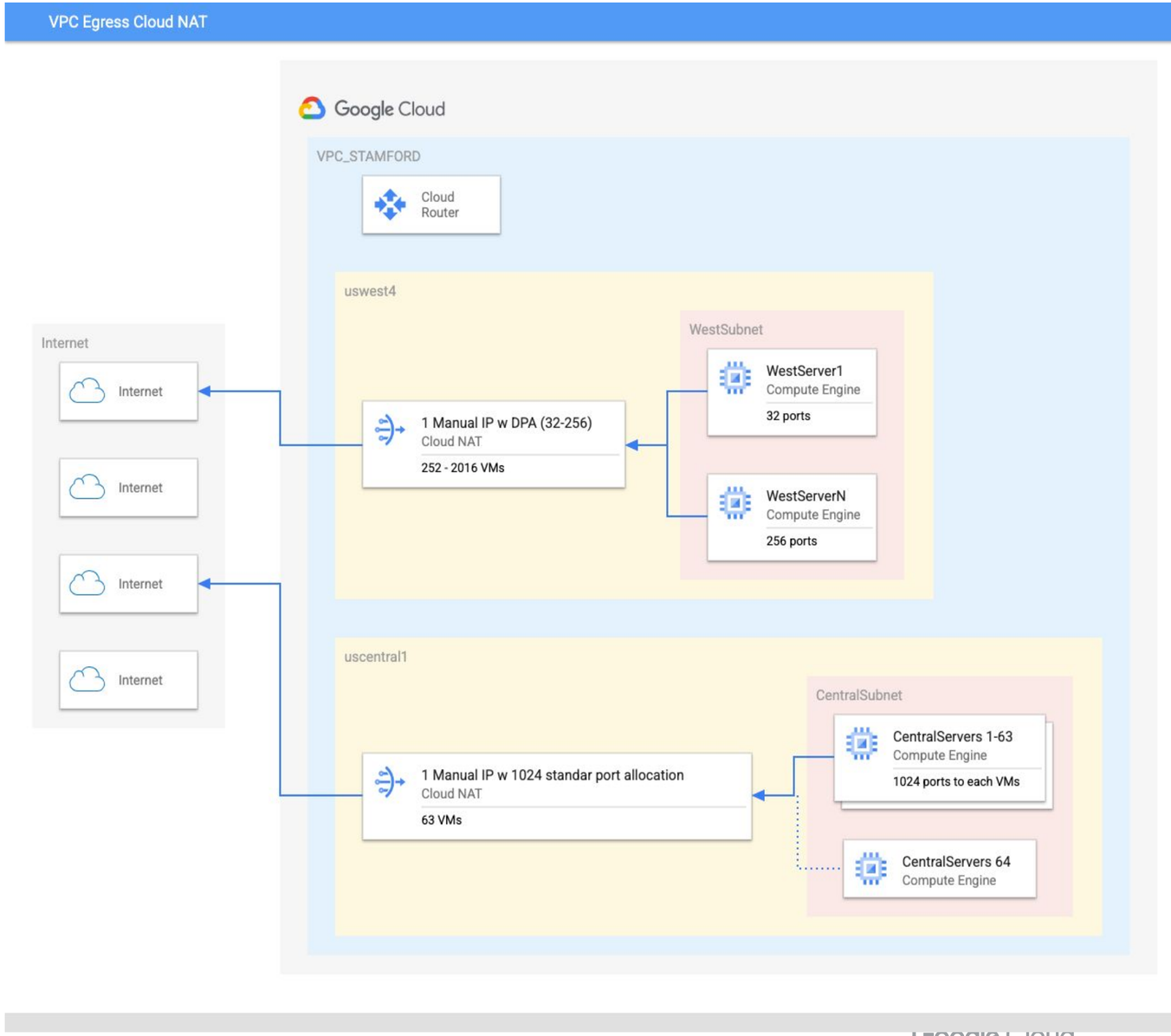
- VMs pre-allocated the same number of ports.

Dynamic Port Allocation (DPA) - Recommended when port exhaustion might be a concern

- Auto scales the number of ports per VM based on the VMs individual usage

Connection Timeouts

- Configurable timeouts for UDP, TCP Idle, TCP TimeWait and ICMP



3.5 Diagnostic Question 08 Discussion

Cymbal is using Cloud NAT to provide internet connectivity to a group of VMs in a subnet. There are 500 VMs in the subnet, and each VM may have up to 1000 internet bound connections simultaneously.

What Cloud NAT configuration will support this requirement?

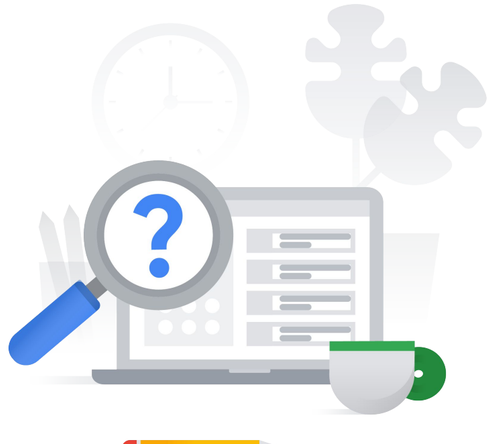
A. Set the minimum ports per VM to 1000, and set the number of IP addresses used by the Cloud NAT Gateway to 8.

B. Set the minimum ports per VM to 2000, and set the number of IP addresses used by the Cloud NAT Gateway to 8.

C. Set the minimum ports per VM to 2000, and set the number of IP addresses used by the Cloud NAT Gateway to 10.

D. Set the minimum ports per VM to 1000, and set the number of IP addresses used by the Cloud NAT Gateway to 6.

3.5 Diagnostic Question 08 Discussion



Cymbal is using Cloud NAT to provide internet connectivity to a group of VMs in a subnet. There are 500 VMs in the subnet, and each VM may have up to 1000 internet bound connections simultaneously.

What Cloud NAT configuration will support this requirement?

A. **Set the minimum ports per VM to 1000, and set the number of IP addresses used by the Cloud NAT Gateway to 8.**

B. Set the minimum ports per VM to 2000, and set the number of IP addresses used by the Cloud NAT Gateway to 8.

C. Set the minimum ports per VM to 2000, and set the number of IP addresses used by the Cloud NAT Gateway to 10.

D. Set the minimum ports per VM to 1000, and set the number of IP addresses used by the Cloud NAT Gateway to 6.

Additional content

QUIZ week 2

(the one we went through during the meeting)

Reminder:

- NOT as complex as questions on the exam
- Technical knowledge validation (No business context)

Additional content 1

[READING]

- VPC network overview - Security properties of a VPC network, VPC peering, shared VPC, and firewall rules
- Best practices and reference architectures for VPC design - Network isolation and data encapsulation for N tier application design
- DNS Security Extensions (DNSSEC) overview - Use of DNSSEC
- Manage DNSSEC configuration (especially focus on migrating DNSSEC-signed zones to Cloud DNS)
- Cloud Armor overview - Tip: know which Load Balancers are supported by Cloud Armor; know preview mode
- VPC firewall rules overview
- Identity-Aware Proxy overview
- IAP for on-premises apps
- Hierarchical firewall policies overview - that's another "policy" topic, but it's NOT related to IAM Policies or Organization Policies
- Choosing a load balancer
- Load balancer features - don't try to memorize all, but rather know high-level of most important ones only (proxy/pass-through, protocols, session affinity, security)
- Shared VPC overview
- VPC Network Peering overview
- Choosing a Network Connectivity product

Additional content 2

- Private access options for services - overview of different options to reach GCP APIs and managed services
  a. Private Google Access:
     i. Private Google Access - overview
     ii. Configuring Private Google Access - differenciate between private.googleapis.com and restricted.googleapis.com!
  b. Private Services Access
     i. Private services access - overview
     ii. Configuring private services access
  c. [new service] Private Service Connect, which solves some difficulties (mainly: non-transitivity of VPC Peering for managed services)
     i. Private Service Connect - overview
     ii. How to publish managed services using Private Service Connect
     iii. How to access managed services using Private Service Connect
  d. Serverless VPC Access
     i. How to access VPC resources from serverless services?
     ii. How to configure Serverless VPC Access
- Cloud NAT overview - with special focus on NAT subnet IP ranges and NAT rules.
- [IMPORTANT] VPC Service Controls. What is a service perimeter and perimeter bridge.

Additional content 3

[VIDEOS]

- Great demo of how to centralize network management and set up Shared VPC in GCP: Level Up From Zero Episode 4: Shared VPC
- Private Service Connect (new service that might solve issues with transitivity when Private Google Access / Private Service Access is being used): What is Private Service Connect?
- IAP as a way to control access to your internal apps (most real IAP use-cases in a single video!): Centralize access to your organization's websites with Identity Aware Proxy (IAP)
- If IAP is not granular enough and application-based auth is needed, you can use GCP Identity Platform Learn to add authentication and identity management to your own apps
- How do I protect my applications from DDoS attacks with Google Cloud Armor?
- Learn about Serverless VPC Connector: Connecting to private GCE instances
- Learn to isolate containerized workloads with Google Cloud - Superb video explaining GKE Sandbox in 5 mins
- How do I provide organizational wide security control using Hierarchical Firewall Policies

[PODCASTS]

- Preparing for Cloud Migrations from a CISO Perspective, Part 2
- Scaling Google Kubernetes Engine Security

Make sure to…

Enjoy the journey as much as the destination!