Google Cloud

Networking in Google Cloud

Controlling access to
VPC Networks

Today's agenda

Use case: Granting access

Least privilege

Sarah

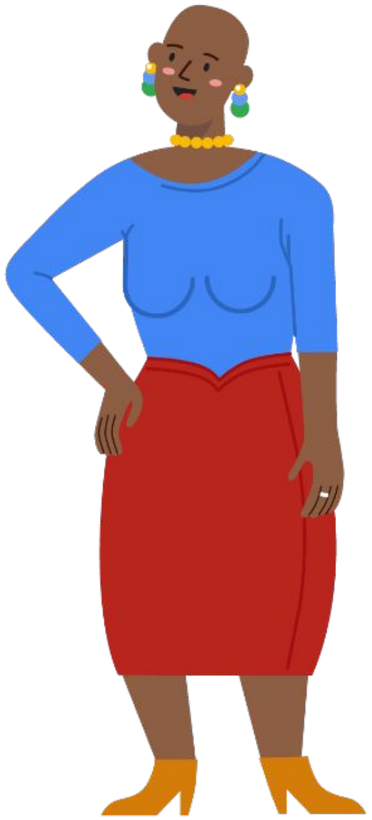
Update VPC network firewall rules.

Jamal

Track user access to networking resources

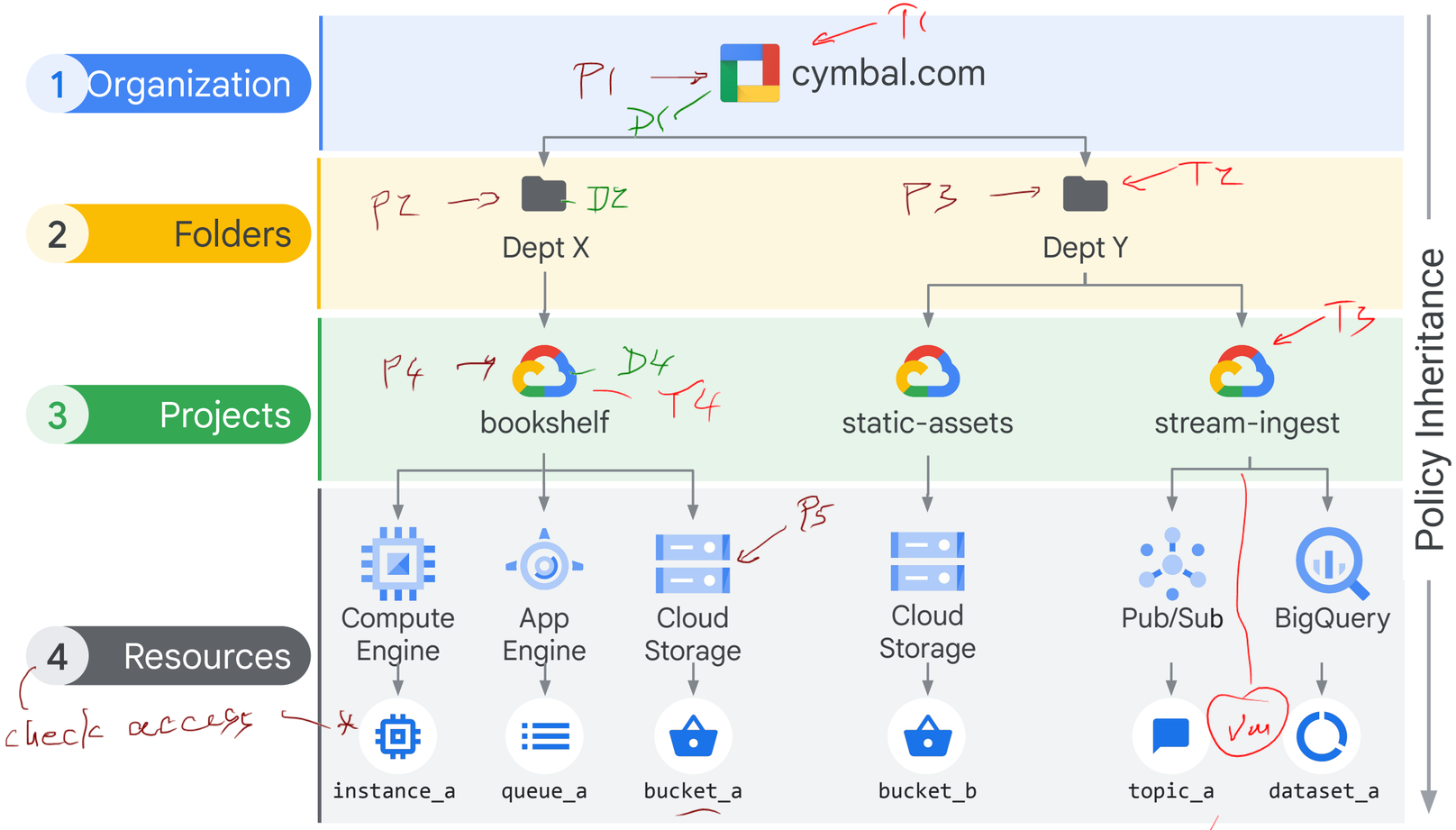
Kalani

View VPC configuration

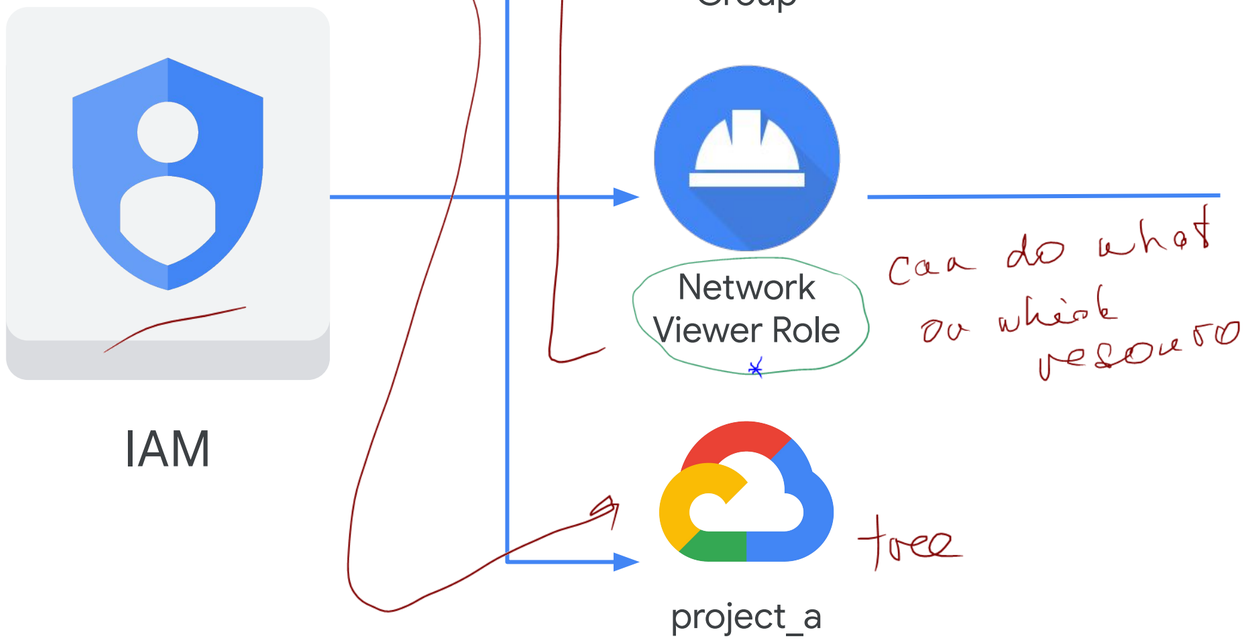


IAM resource hierarchy

- A policy is set on a resource, and each policy contains a set of:
  - Roles
  - Members
- Resources inherit policies from the parent.
- A less restrictive parent policy will override a more restrictive child resource policy.
- A deny policy can be used to further restrict access.



Predefined roles



List of Permissions

- ✓ compute.addresses.get
- ✓ compute.addresses.list
- ✓ compute.globalAddresses.get
- ✓ compute.globalAddresses.list
- ✓ compute.backendBuckets.get
- ✓ compute.backendBuckets.list
- ✓ compute.networks.list

...

Custom roles

List of Permissions

- ✓ Compute.firewalls.
- ✓ compute.sslCertificates.get
- ✓ compute.sslCertificates.list

Custom Role

My Network Admin Role

IAM

Network-related IAM roles

separation of duties

Role title	Description
Network viewer	Read-only access to all networking resources
Network administrator	Permission to create, modify, and delete networking resources, except for firewall rules and SSL certificates
Security administrator	Permission to create, modify, and delete firewall rules and SSL certificates not networks

Use case: Granting access

Sarah

Update VPC network firewall rules.

Predefined network administrator

Jamal

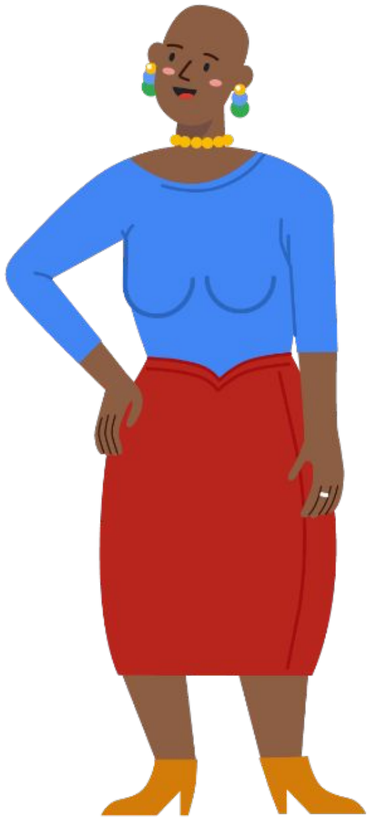
Track user access to networking resources

Custom role: log viewer for networking resources

Kalani

View VPC configuration

Predefined network viewer



Today's agenda

01 IAM roles

02 Firewall rules

03 Lab: Configuring VPC Firewalls

04 Cloud IDS

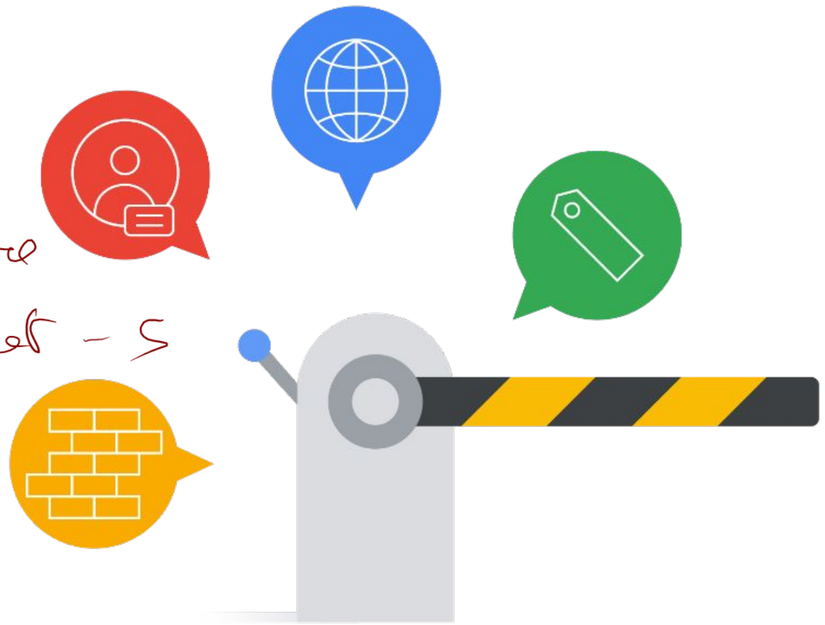
05 Lab: Getting Started with Cloud IDS

06 Secure Web Proxy

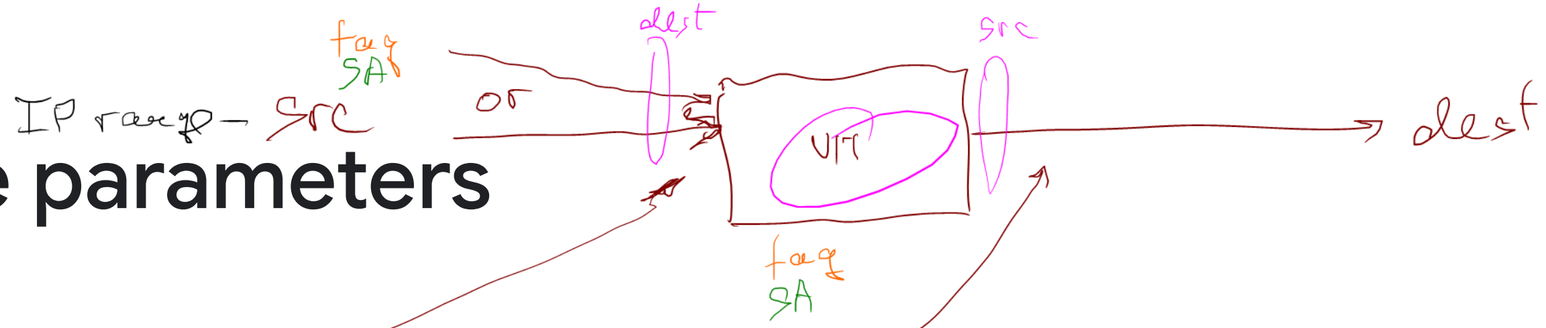
07 Quiz

Firewall rules can be applied to your network and resources in several ways

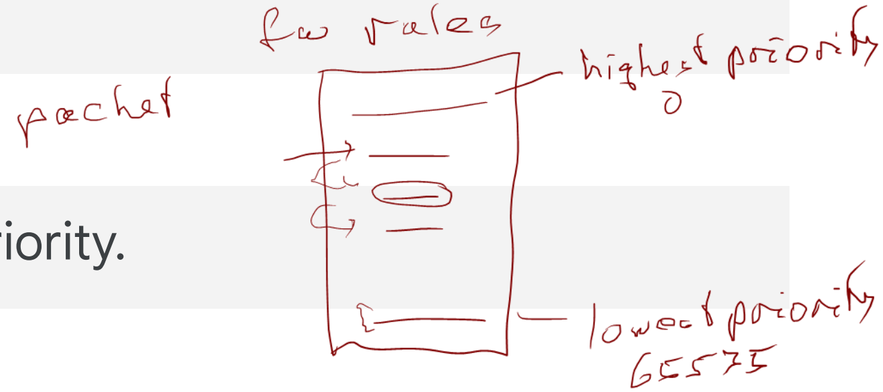
- All instances in the network.
- Instances with a specific target tag.
- Instances using a specific service account.
- Firewall rules are “stateful.”
- To apply firewall rules to multiple VPC networks in an organization, use firewall policies.
- Firewall policies use tags to identify and group resources for firewall rules.



Firewall rule parameters



Parameter	Details
Direction	Ingress or egress
Source or destination	The source parameter is only applicable to ingress rules.
	The destination parameter is only applicable to egress rules.
Protocol and port	Rules can be restricted to specific protocols only, or combinations of protocols and ports only.
Action	Allow or deny
Priority	0–65535. A lower number indicates a higher priority.



All VPCs have implied firewall rules

Implied IPv4 firewall rules are present in all VPC networks

- Implied IPv4 allow egress rule: Lets any instance send traffic to any destination.
- Implied IPv4 deny ingress rule: Protects all instances by blocking incoming connections to them.

If IPv6 is enabled, the VPC network also has these two implied rules:

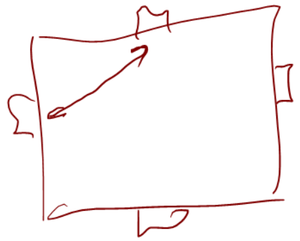
- Implied IPv6 allow egress rule: Lets any instance send traffic to any destination.
- Implied IPv6 deny ingress rule: Protects all instances by blocking incoming connections to them.

Default VPCs have additional allow rules

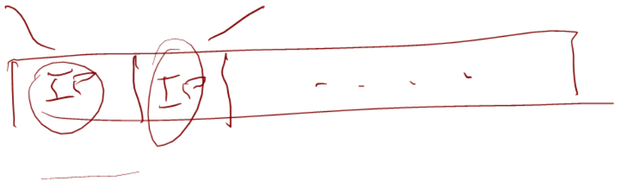
Rule	Description
`default-allow-internal`	Allows ingress connections for all protocols and ports among instances within the VPC network.
`default-allow-ssh`	Allows port 22 - secure shell (ssh) access.
`default-allow-rdp`	Allows port 3389 - remote desktop protocol (RDP) access.
`default-allow-icmp`	Allows ICMP traffic.

Some VPC network traffic is always allowed

- Packets sent to and received from the Google Cloud metadata server.
- Packets sent to an IP address assigned to one of the instance's own network interfaces (NICs) where packets stay within the VM itself.



Some VPC network traffic is always blocked

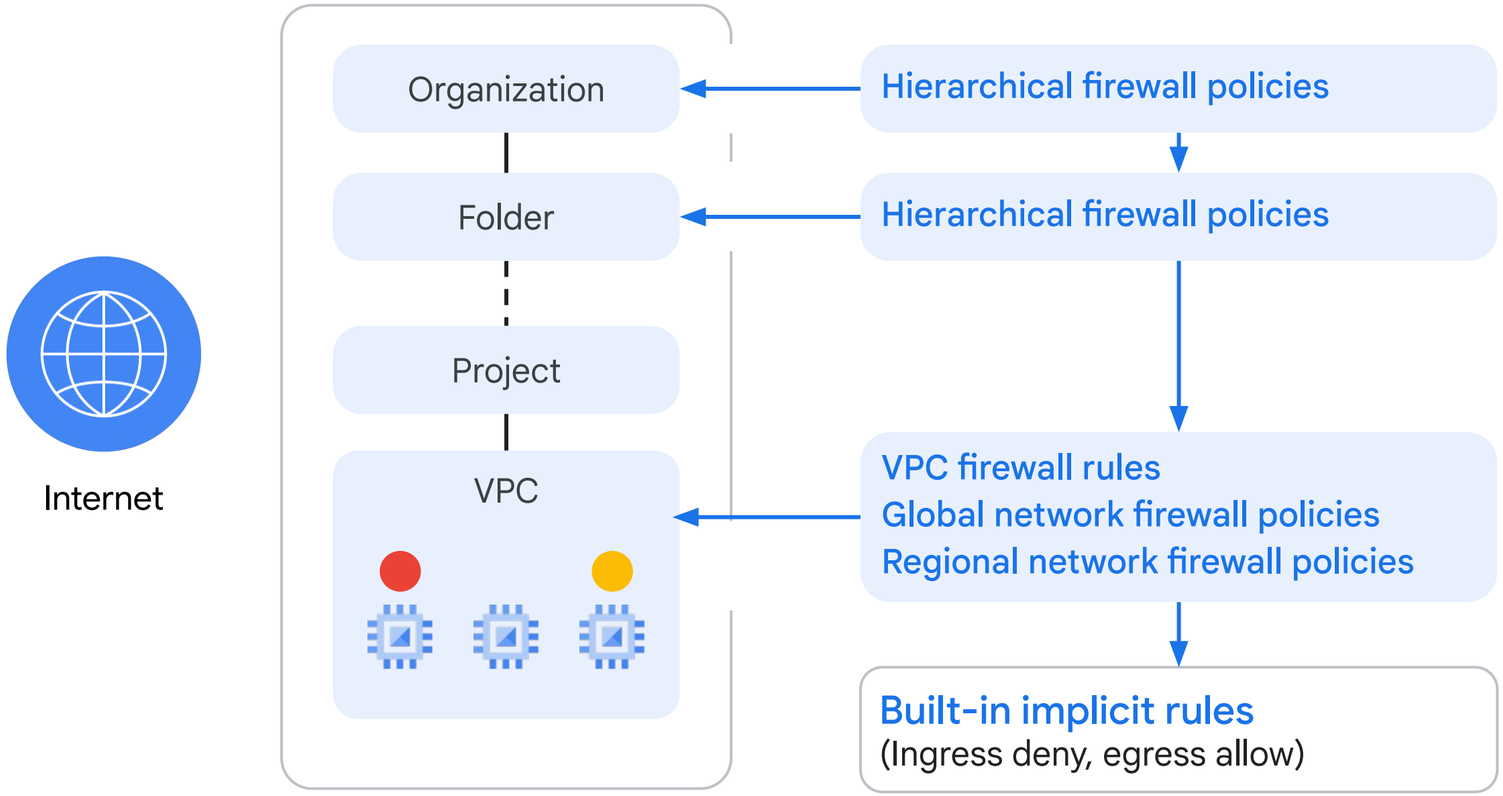


Blocked traffic	Applies to
DHCP offers and acknowledgments	Ingress packets to UDP port 68 (DHCPv4) Ingress packets to UDP port 546 (DHCPv6)
All traffic other than external IPv4 and IPv6 using protocols TCP, UDP, ICMP, ICMPv6, IPIP, AH, ESP, SCTP, and GRE	Ingress packets to external IP addresses

Firewall rule best practices

1. Use the model of least privilege.
2. Minimize direct exposure to/from the internet.
3. Prevent ports and protocols from being exposed unnecessarily.
4. Develop a standard naming convention for firewall rules. For example:
   - `{direction}-{allow/deny}-{service}-{to-from-location}`
   - `Ingress-allow-ssh-from-onprem`
   - `egress-allow-all-to-gcevms`
5. Consider service account firewall rules instead of tag-based rules.

Hierarchical, global, and regional network firewall policies



Hierarchical firewall policies can apply to many VPC networks in one or many projects.

Global network firewall policies can apply to resources across a VPC network.

Regional network firewall policies can apply to resources in a region in a VPC network.

Firewall Insights helps you better understand and safely optimize your firewall rules

Cloud Monitoring:
Metrics

Network Intelligence Center
Firewall Insights

Recommender:
Insights

Use case: Apply firewall rules hierarchically

Requirements:

A firewall solution that can be applied at multiple levels

Solution:

Cloud Firewall

- Organization firewall policy
- Folder firewall policy
- VPC firewall rules
- Network firewall policy
- Built-in implicit rules (ingress deny, egress allow)

Today's agenda

01 IAM roles

02 Firewall rules

03 Lab: Configuring VPC Firewalls

04 Cloud IDS

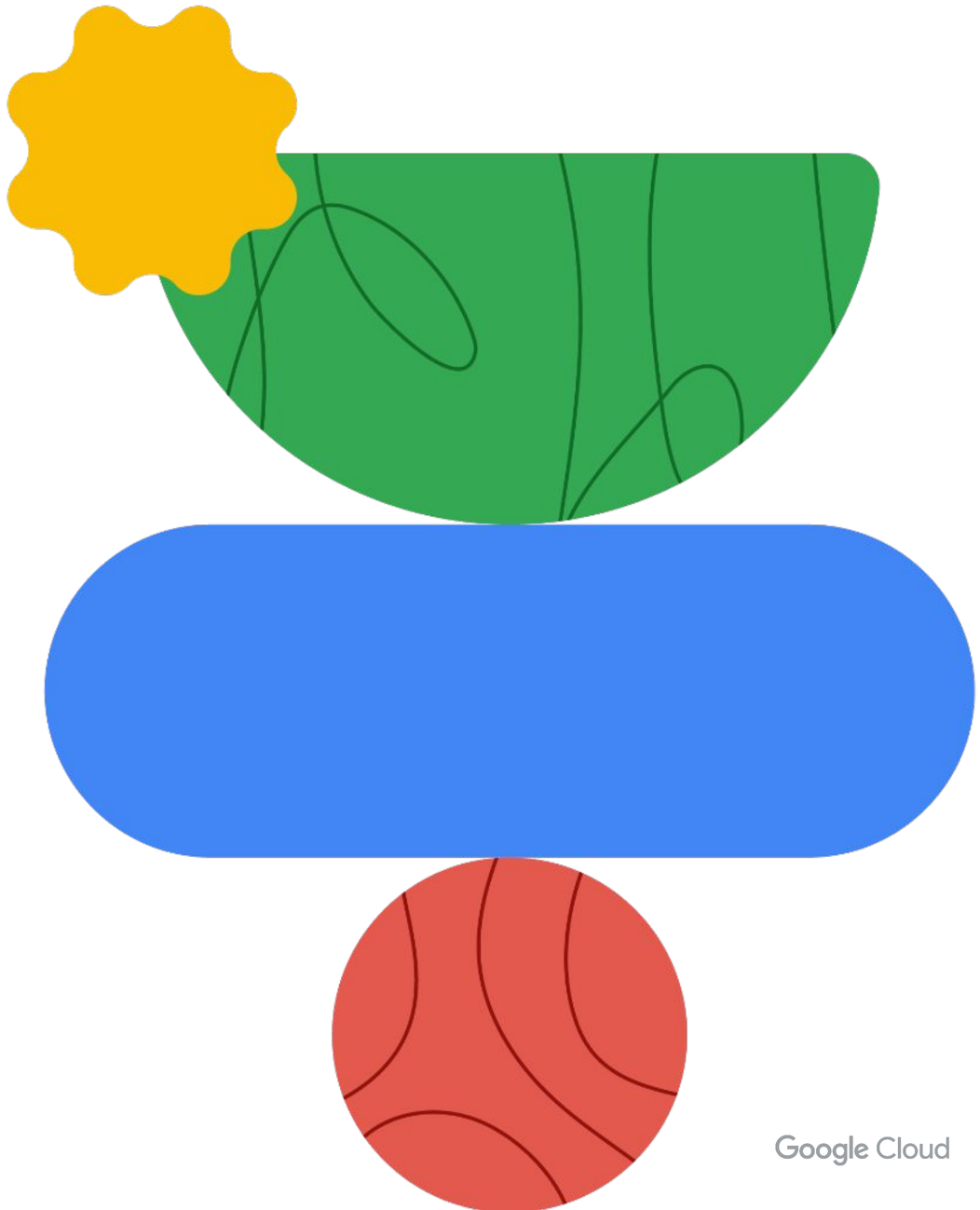
05 Lab: Getting Started with Cloud IDS

06 Secure Web Proxy

07 Quiz

Lab

Configuring VPC Firewalls



Today's agenda

01 IAM roles

02 Firewall rules

03 Lab: Configuring VPC Firewalls

04 Cloud IDS

05 Lab: Getting Started with Cloud IDS

06 Secure Web Proxy

07 Quiz

Use case: Detect network-based threats

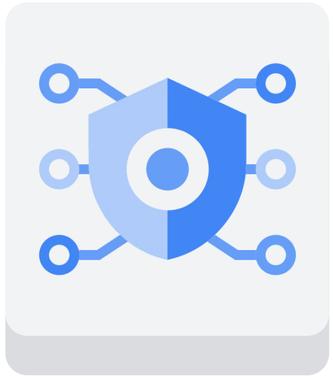
Problem:

- Unauthorized access attempts
- Execution of malicious software
- Covert monitoring tools, and command-and-control attacks

Solution: Cloud IDS

- Cloud IDS is a network security service offered by Google Cloud.
- It provides improved visibility into network and system vulnerabilities.
- It has threat detection capabilities.

Cloud IDS: Overview



It provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network.

Creates a Google-managed peered network with mirrored VMs.

Inspects traffic from mirrored VMs to provide advanced threat detection.

Provides full visibility into network traffic, letting you monitor VM-to-VM communication.

Meets your advanced threat detection and compliance requirements, including PCI 11.4.

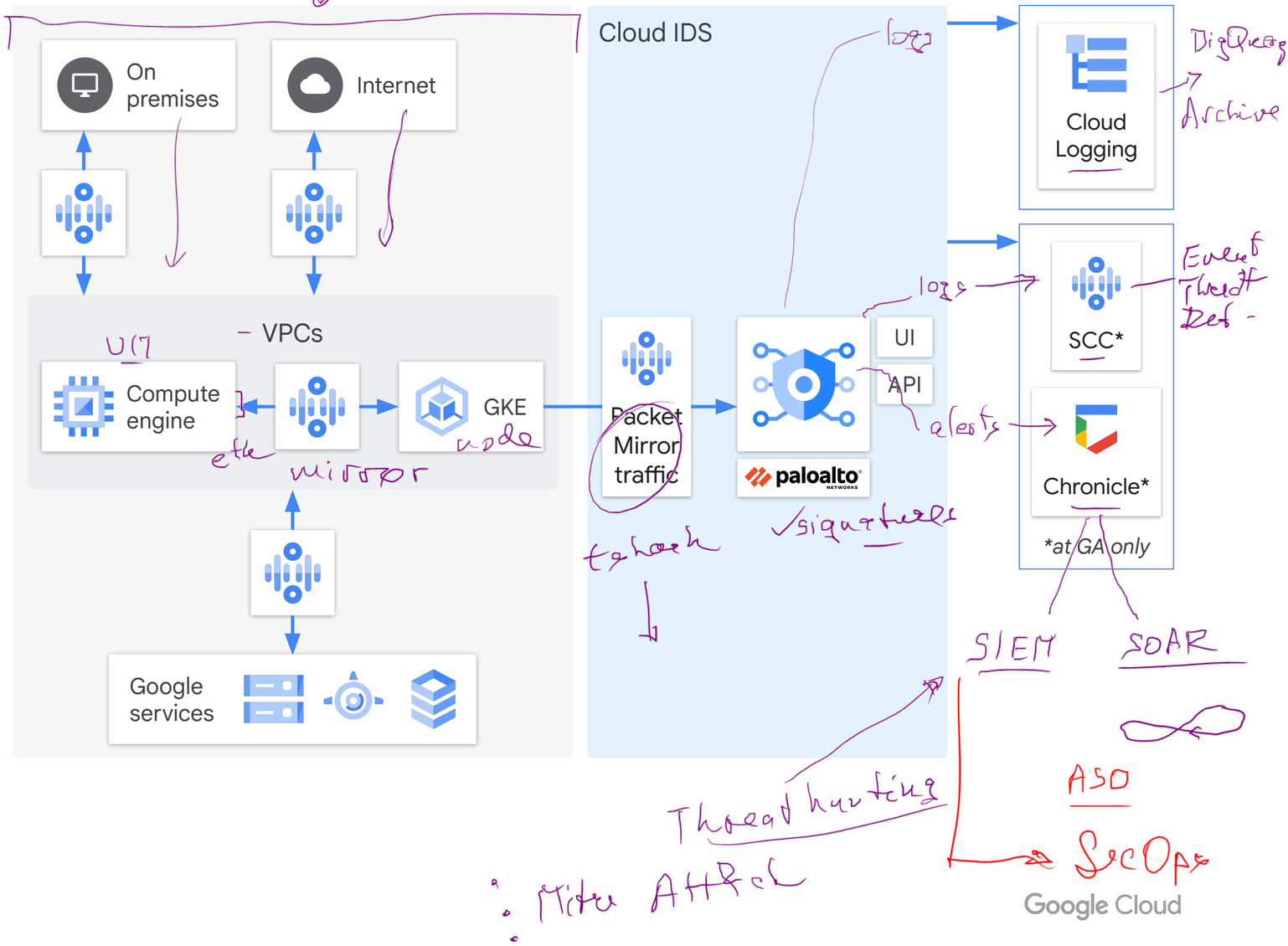
Cloud IDS: Endpoints and packet mirroring

IDS endpoint

- Zonal resource that inspects traffic from any zone in its region.
- Receives mirrored traffic and performs threat detection analysis.

Packet mirroring

- Creates a copy of your network traffic.
- Attaches packet mirroring policies to IDS endpoints.



Today's agenda

01 IAM roles

02 Firewall rules

03 Lab: Configuring VPC Firewalls

04 Cloud IDS

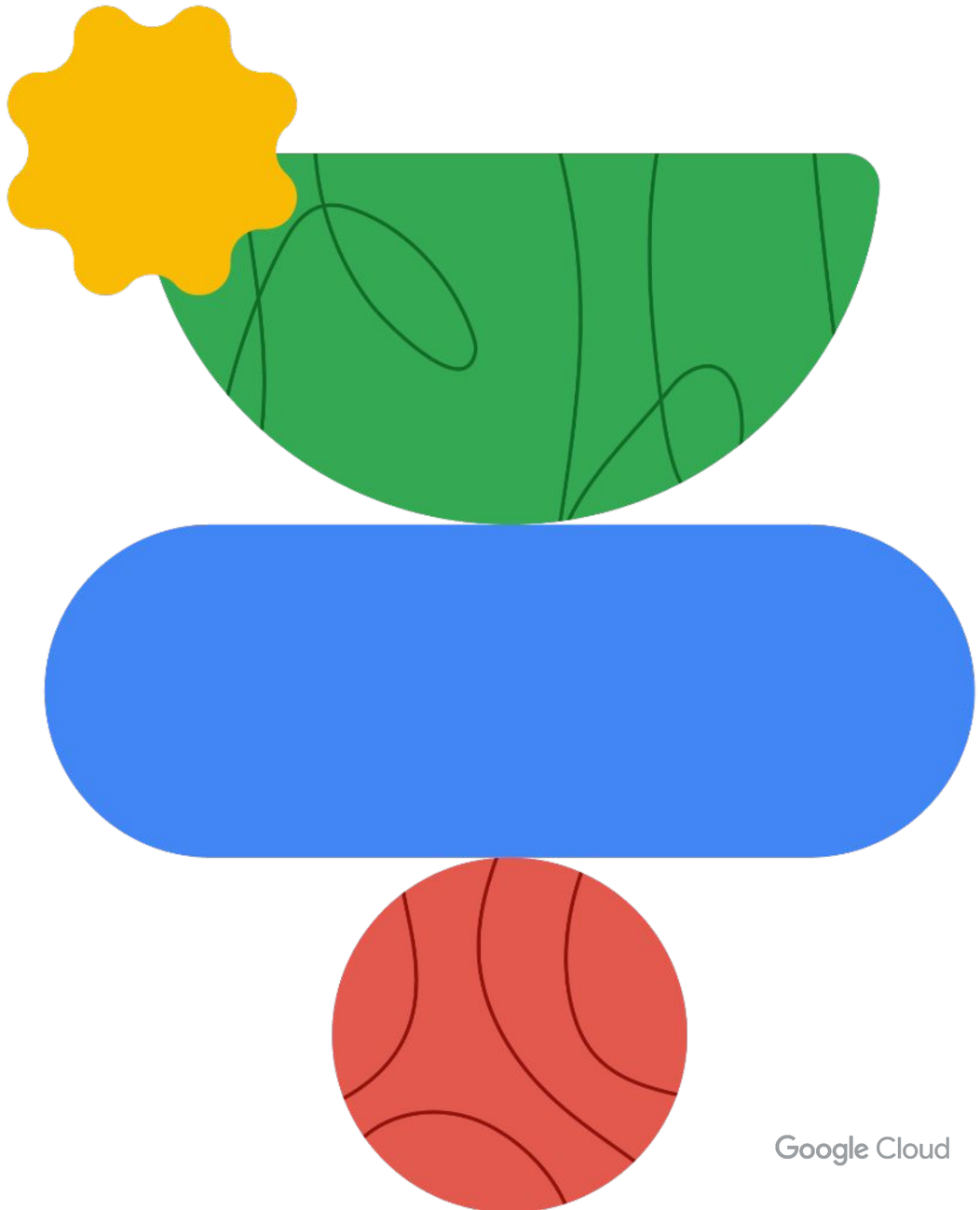
05 Lab: Getting Started with Cloud IDS

06 Secure Web Proxy

07 Quiz

Lab intro

Getting Started with Cloud IDS



Today's agenda

01 IAM roles

02 Firewall rules

03 Lab: Configuring VPC Firewalls

04 Cloud IDS

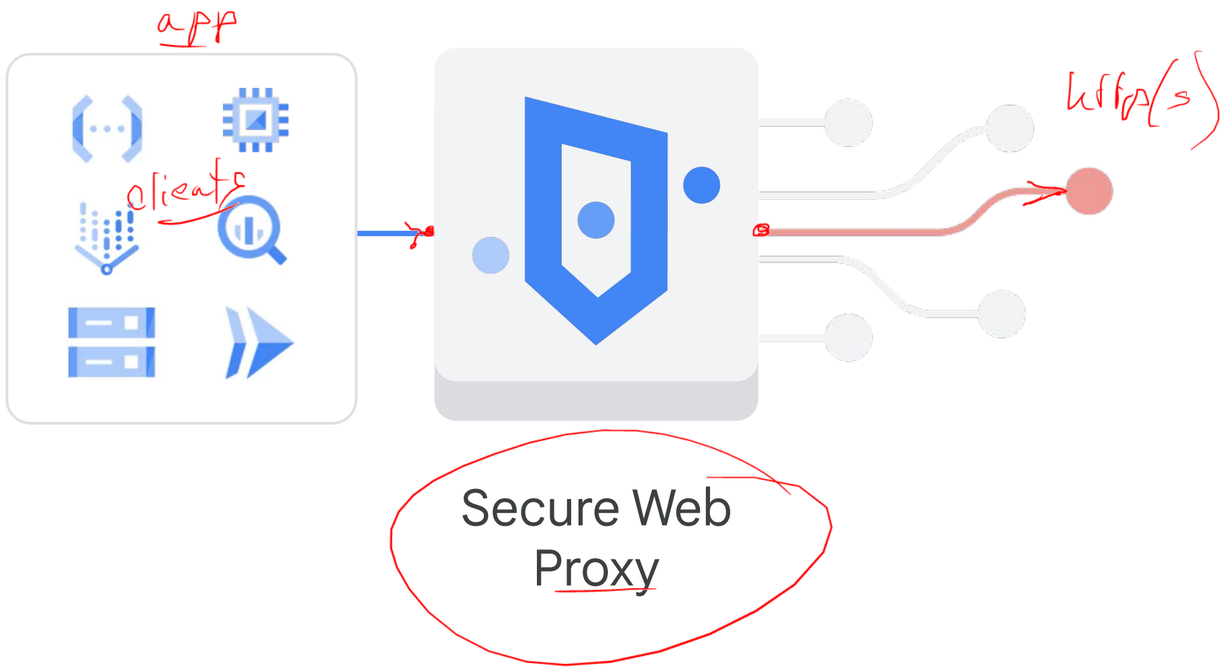
05 Lab: Getting Started with Cloud IDS

06 Secure Web Proxy

07 Quiz

Restrict access to trusted external web services

- Secure Web Proxy enhances the security of outbound web traffic from different sources.
- Secure Web Proxy acts as a gateway to filter traffic based on configurable policies.



Common use cases

Cloud migration

Simplifies the transition to Google Cloud by maintaining your current security policies for outbound web traffic.

Egress control

Granular policies (Identity and URL centric) for web traffic to Internet.

Incident forensics

Investigate security events and incidents of any kind related to web traffic and internet via comprehensive logging.

Use case: Restrict access to trusted external web services

- Secure Web Proxy allows you to create very specific rules for outgoing web traffic from your cloud environment.
- Secure Web Proxy can significantly increase the security of your network.
- Secure Web Proxy is a proactive approach to cyber security.

Today's agenda

01 IAM roles

02 Firewall rules

03 Lab: Configuring VPC Firewalls

04 Cloud IDS

05 Lab: Getting Started with Cloud IDS

06 Secure Web Proxy

07 Quiz

Quiz | Question 1

Question

Which IAM role includes permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates?

A. Network administrator

B. Network viewer

C. Security administrator

D. Security viewer

Quiz | Question 1

Answer

Which IAM role includes permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates?

A. Network administrator 

B. Network viewer

C. Security administrator

D. Security viewer

Quiz | Question 2

Question

Which type of IAM member belongs to an application or virtual machine instead of an individual end user?

A. Google account

B. Service account

C. Google group

D. Cloud Identity domain

Quiz | Question 2

Answer

Which type of IAM member belongs to an application or virtual machine instead of an individual end user?

A. Google account

B. Service account 

C. Google group

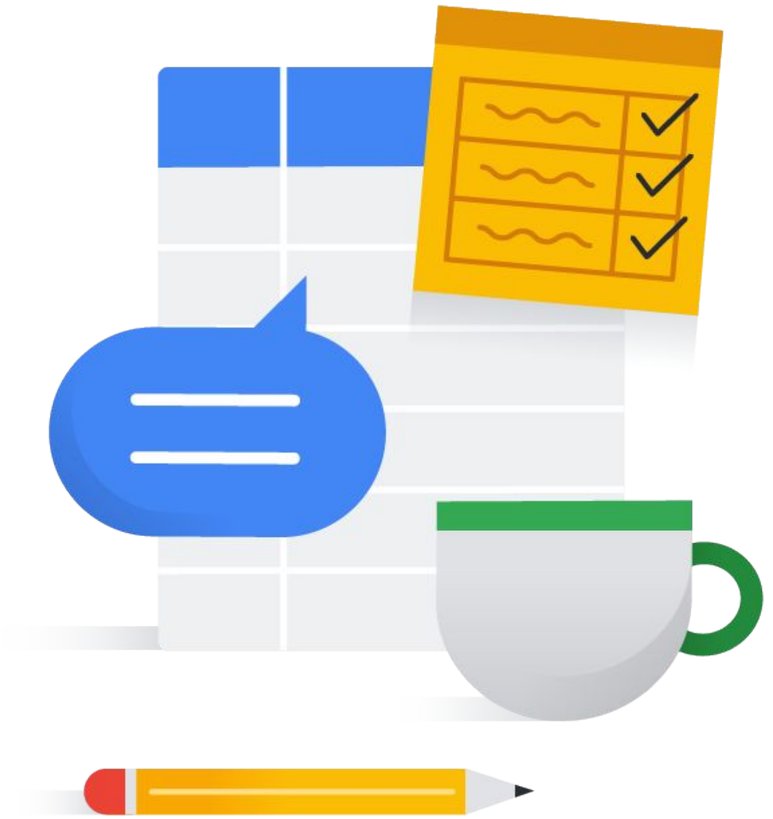
D. Cloud Identity domain

Let’s ask Gemini

How do I optimize IAM permissions?

Create a gcloud command to give the developer Google group access to view my Google Cloud project.

Debrief



Thank you.