Google Cloud

Networking in Google Cloud

Network Monitoring and Logging

Today’s agenda

01 Monitoring

02 Lab: Resource Monitoring

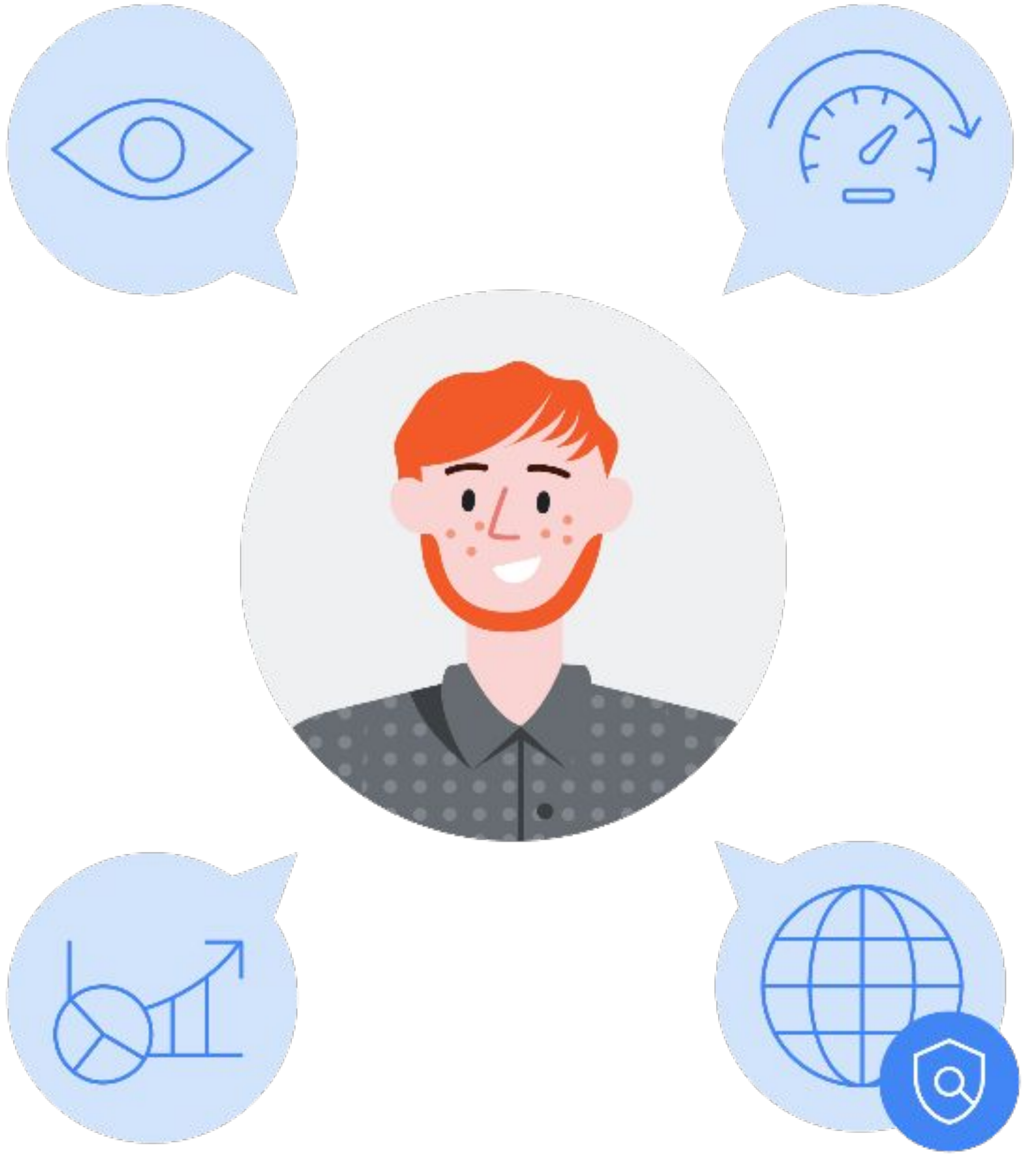
03 Logging

04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

Use case: Visualize and monitor a complex network

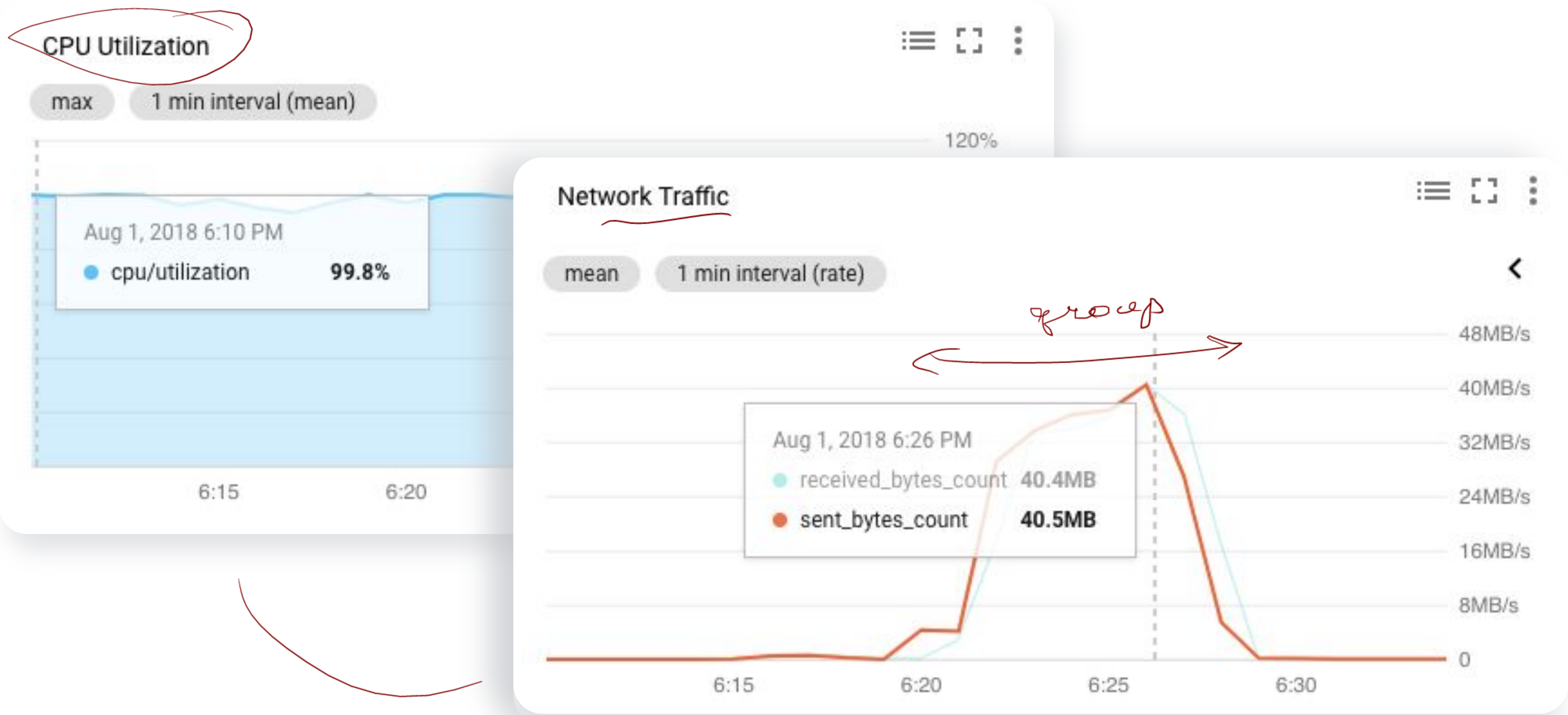
- Tal is a cloud network engineer at Cymbal, where networks are incredibly large and complex.
- Tal has challenges
  - Maintaining **visibility** into the network.
  - Ensuring **optimal network performance.**
  - Identifying bottlenecks and **connectivity issues.**
  - Analyzing and viewing **network insights.**
- How can Tal utilize the comprehensive set of tools by Google Cloud to monitor the network?



custom

Dashboards can show utilization and network traffic

metrics + custom
events
metadata


CPU Utilization

max | 1 min interval (mean)

Aug 1, 2018 6:10 PM
● cpu/utilization 99.8%

Network Traffic

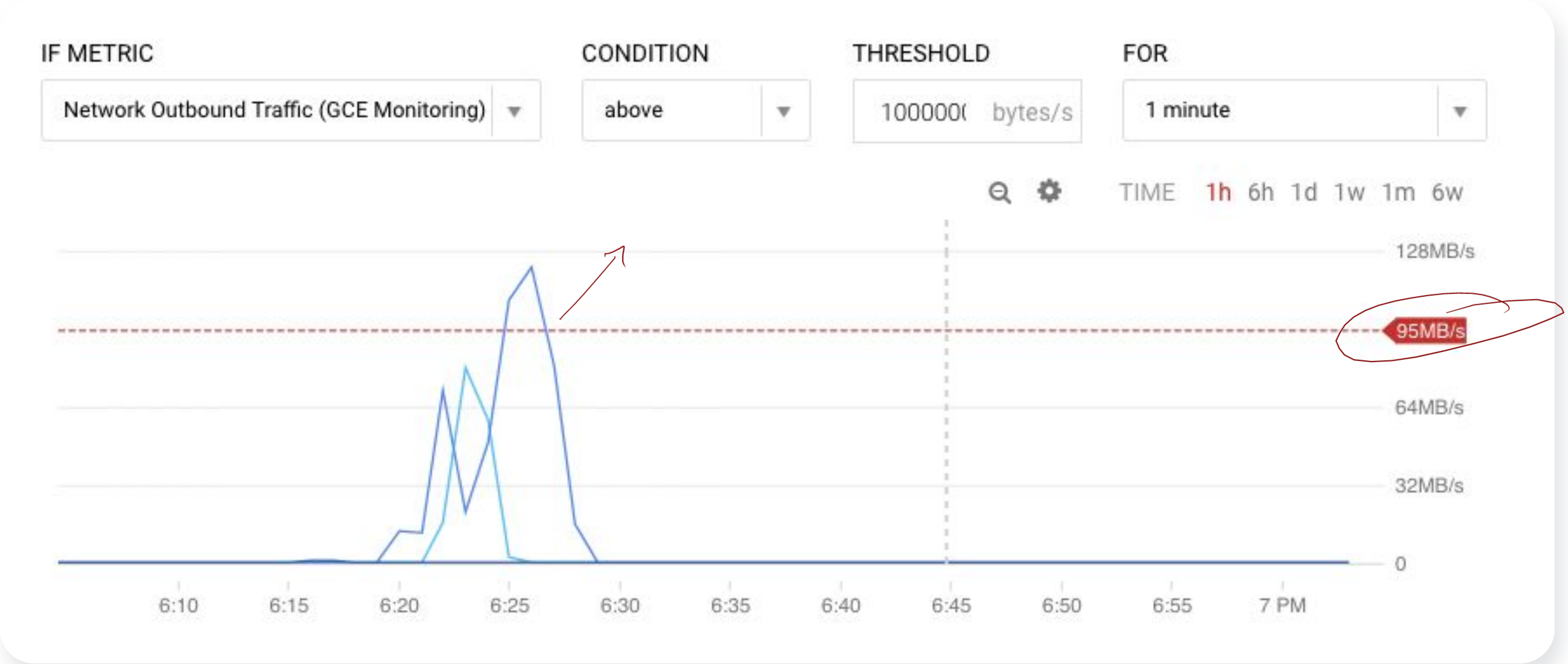
mean | 1 min interval (rate)

Aug 1, 2018 6:26 PM
● received_bytes_count 40.4MB
● sent_bytes_count 40.5MB

group

charts
+ custom — filters

Alerting policies can notify you of certain conditions



IF METRIC

Network Outbound Traffic (GCE Monitoring) ▾

CONDITION

above ▾

THRESHOLD

100000(bytes/s

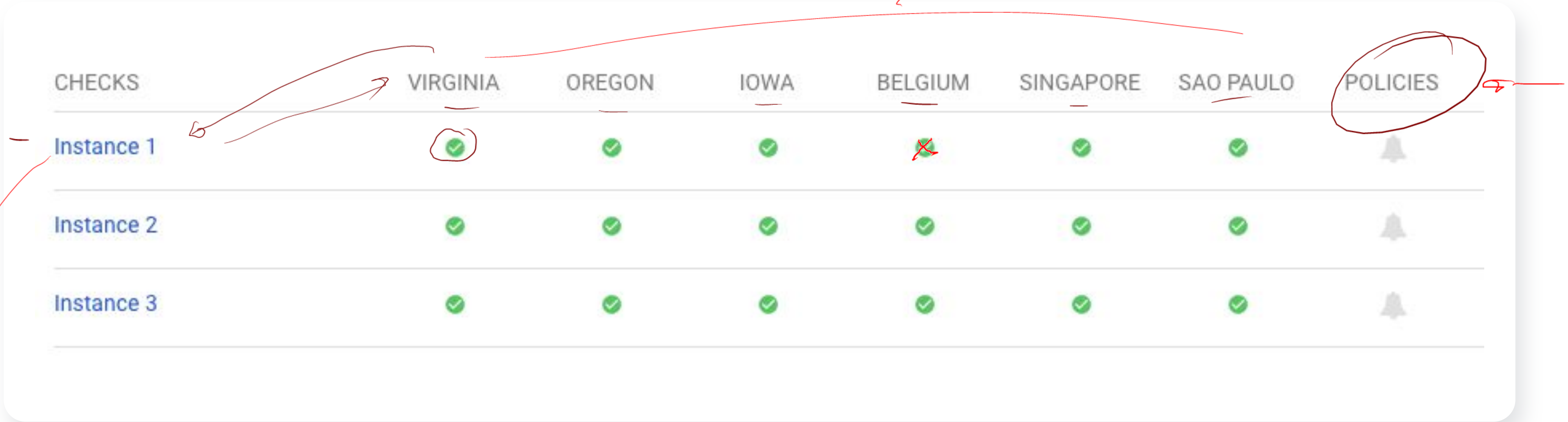
FOR

1 minute ▾

Uptime checks test the availability of your public services

monitor - reactive

60 sec



CHECKS	VIRGINIA	OREGON	IOWA	BELGIUM	SINGAPORE	SAO PAULO	POLICIES
Instance 1	✓	✓	✓	✓	✓	✓	🔔
Instance 2	✓	✓	✓	✓	✓	✓	🔔
Instance 3	✓	✓	✓	✓	✓	✓	🔔

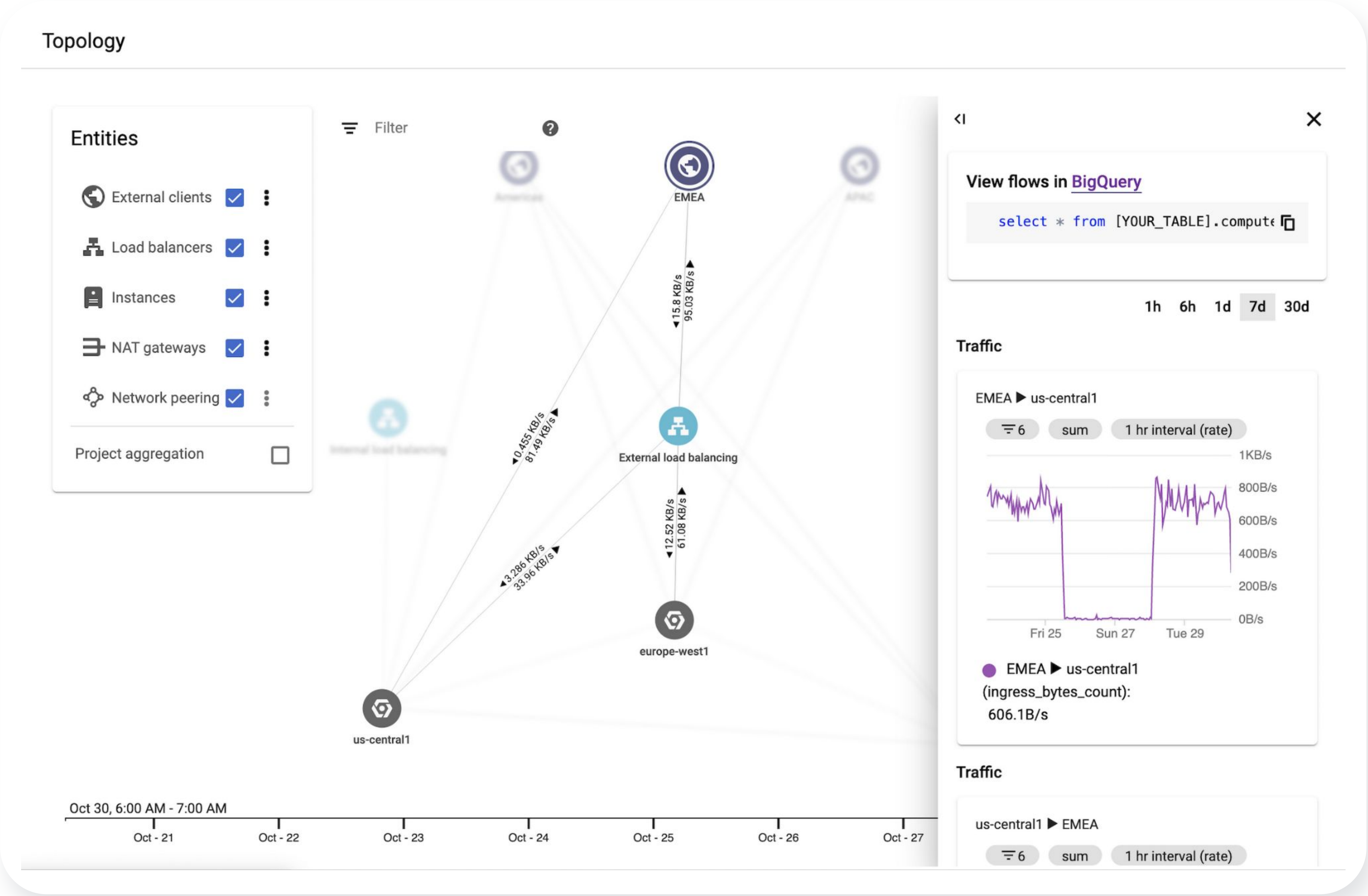
app -

logs

@ 10 sec

* Network Intelligence Center

proactive



Topology

Entities

- External clients ☑
- Load balancers ☑
- Instances ☑
- NAT gateways ☑
- Network peering ☑

Project aggregation □

View flows in BigQuery

```
select * from [YOUR_TABLE].compute
```

1h 6h 1d 7d 30d

Traffic

EMEA ▶ us-central1

6 sum 1 hr interval (rate)

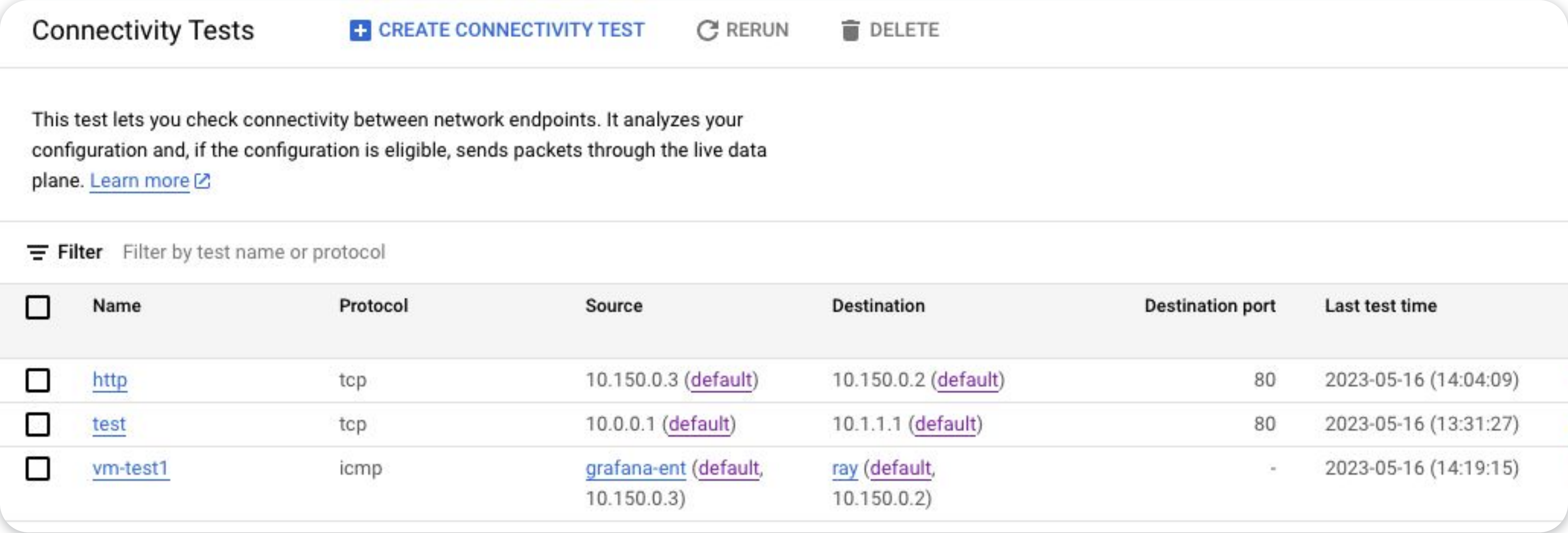
● EMEA ▶ us-central1 (ingress_bytes_count): 606.1B/s

Traffic

us-central1 ▶ EMEA

6 sum 1 hr interval (rate)

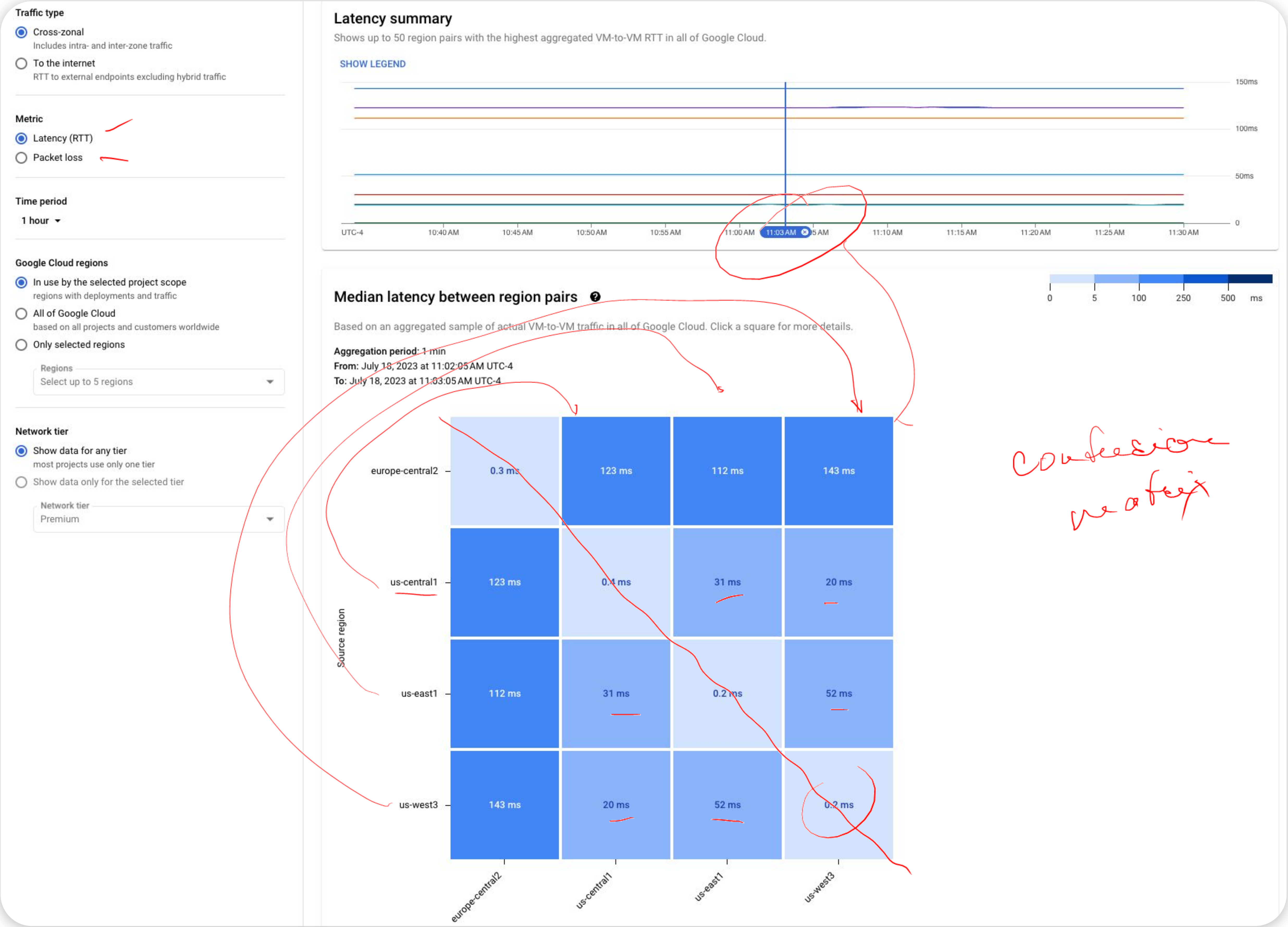
Diagnose issues using Connectivity Tests



This test lets you check connectivity between network endpoints. It analyzes your configuration and, if the configuration is eligible, sends packets through the live data plane. Learn more

□	Name	Protocol	Source	Destination	Destination port	Last test time
□	http	tcp	10.150.0.3 (default)	10.150.0.2 (default)	80	2023-05-16 (14:04:09)
□	test	tcp	10.0.0.1 (default)	10.1.1.1 (default)	80	2023-05-16 (13:31:27)
□	vm-test1	icmp	grafana-ent (default, 10.150.0.3)	ray (default, 10.150.0.2)	-	2023-05-16 (14:19:15)

Performance Dashboard



Traffic type

● Cross-zonal
Includes intra- and inter-zone traffic

○ To the internet
RTT to external endpoints excluding hybrid traffic

Metric

● Latency (RTT)

○ Packet loss

Time period

1 hour ▾

Google Cloud regions

● In use by the selected project scope
regions with deployments and traffic

○ All of Google Cloud
based on all projects and customers worldwide

○ Only selected regions

Regions
Select up to 5 regions ▾

Network tier

● Show data for any tier
most projects use only one tier

○ Show data only for the selected tier

Network tier
Premium ▾

Latency summary

Shows up to 50 region pairs with the highest aggregated VM-to-VM RTT in all of Google Cloud.

SHOW LEGEND

Median latency between region pairs

Based on an aggregated sample of actual VM-to-VM traffic in all of Google Cloud. Click a square for more details.

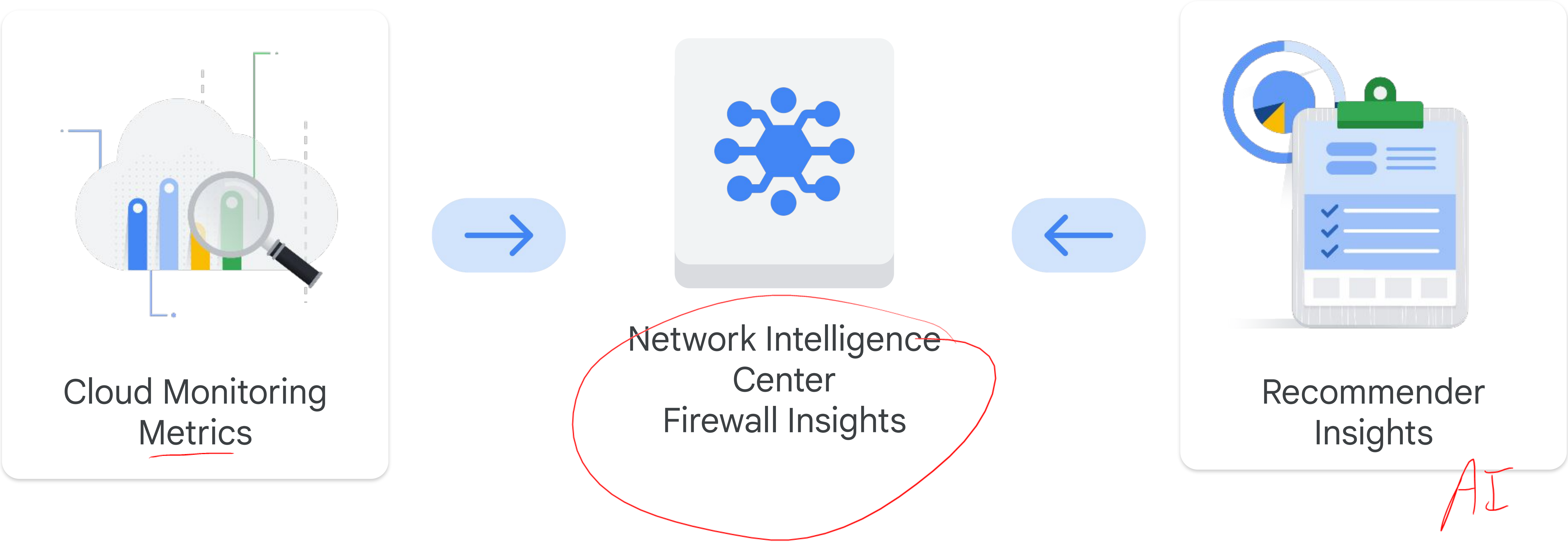
Aggregation period: 1 min
From: July 18, 2023 at 11:02:05 AM UTC-4
To: July 18, 2023 at 11:03:05 AM UTC-4

Source region	europe-central2	us-central1	us-east1	us-west3
europe-central2	0.3 ms	123 ms	112 ms	143 ms
us-central1	123 ms	0.4 ms	31 ms	20 ms
us-east1	112 ms	31 ms	0.2 ms	52 ms
us-west3	143 ms	20 ms	52 ms	0.2 ms

confusione
ma a fey

Firewall Insights

- Help you understand and optimize firewall configurations.
- Let you view reports on firewall usage and the impact of rules on VPC.



Cloud Monitoring Metrics

Network Intelligence Center Firewall Insights

Recommender Insights

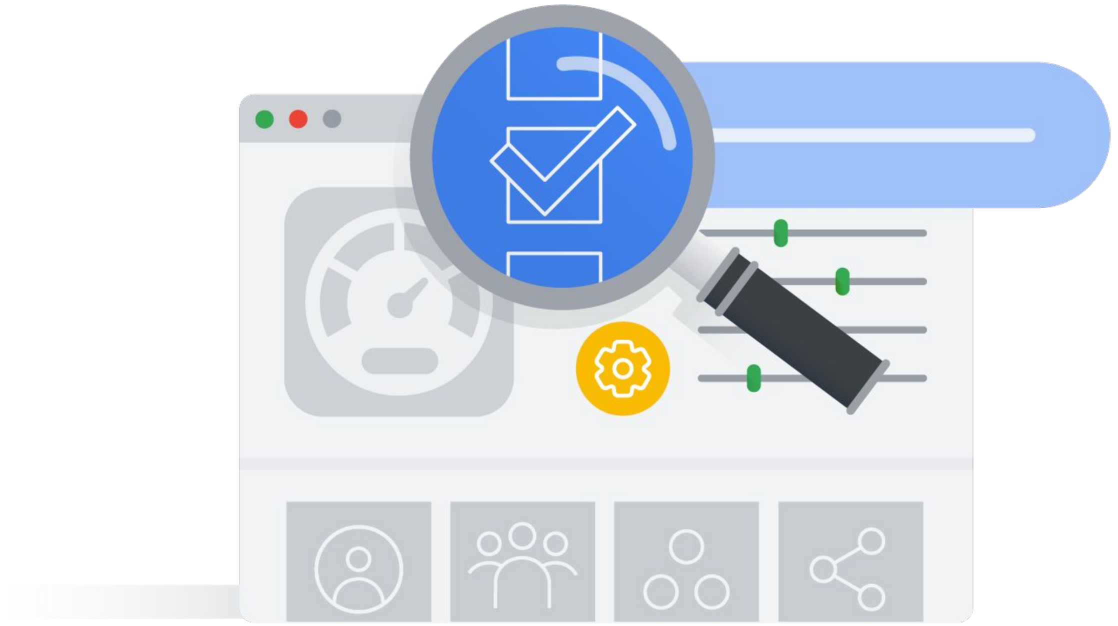
AI

log based

enable fw logging $

Metrics let you analyze the way that your firewall rules are being used

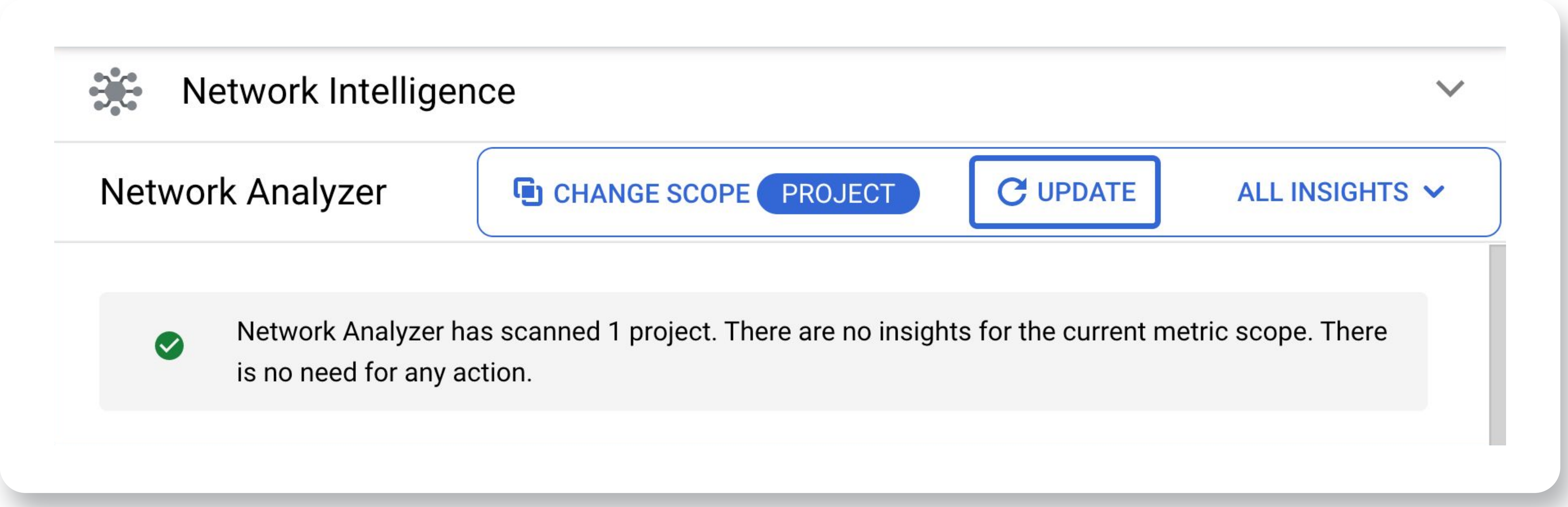
- Analyze firewall usage
- Track firewall behavior
- Diagnose dropped connections
- Identify potential threats



Network Analyzer

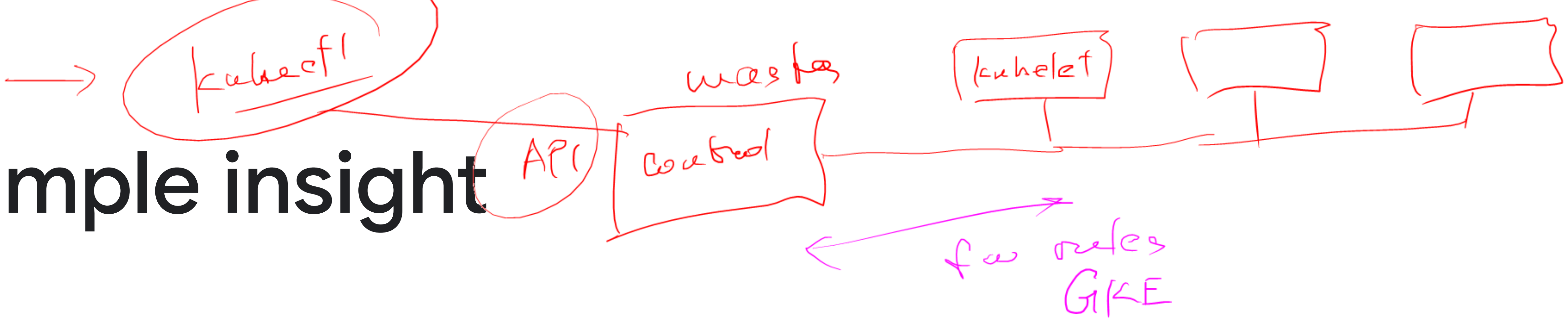
– AI

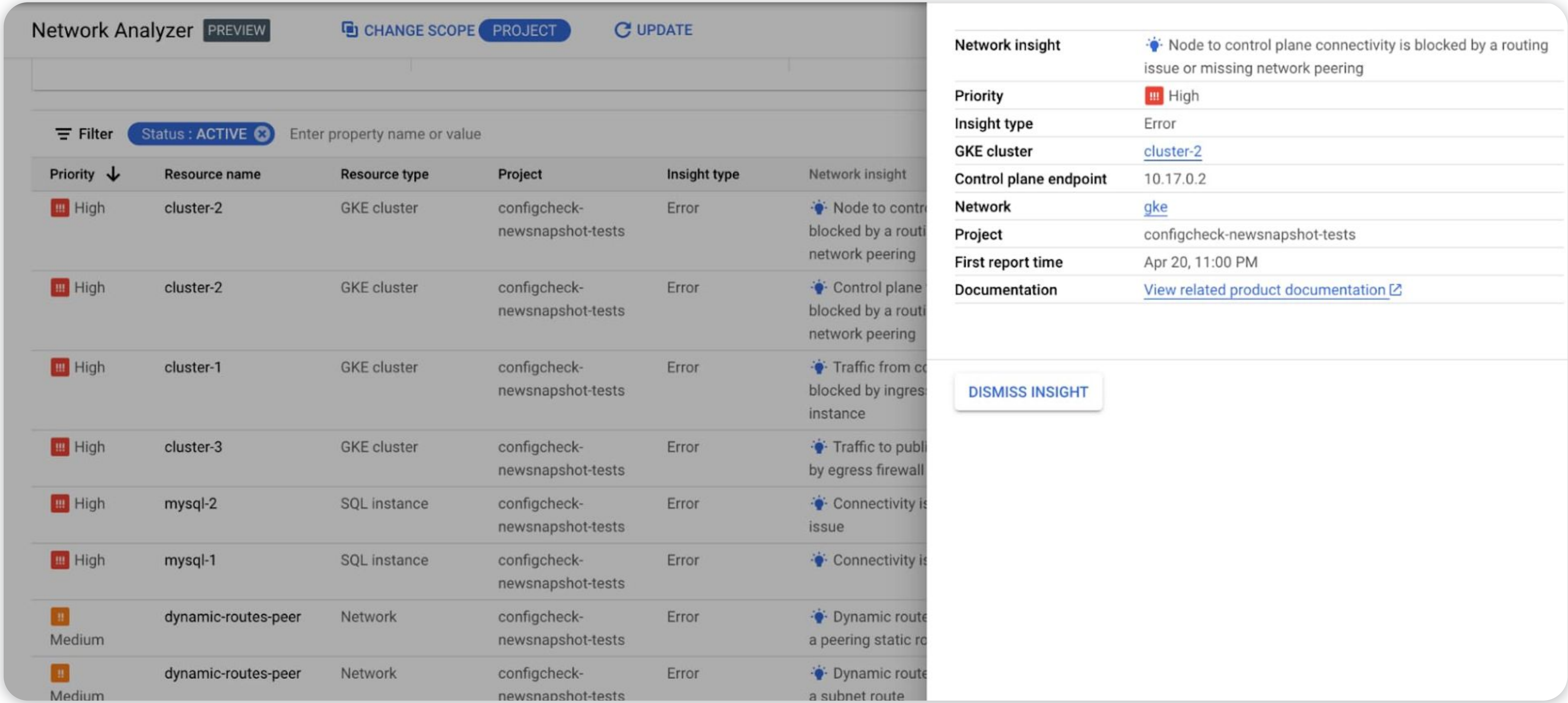
- Automatically monitors your VPC network configurations and detects misconfigurations and suboptimal configurations.
- Provides insights on network topology, firewall rules, routes, configuration dependencies, and connectivity to services and applications.
- Identifies network failures, provides root cause information, and suggests possible resolutions.



Network Analyzer has scanned 1 project. There are no insights for the current metric scope. There is no need for any action.

Network Analyzer sample insight





Network Analyzer PREVIEW   CHANGE SCOPE PROJECT   UPDATE

Filter Status : ACTIVE ⊗ Enter property name or value

Priority ↓	Resource name	Resource type	Project	Insight type	Network insight
High	cluster-2	GKE cluster	configcheck-newsnapshot-tests	Error	Node to contr blocked by a routi network peering
High	cluster-2	GKE cluster	configcheck-newsnapshot-tests	Error	Control plane blocked by a routi network peering
High	cluster-1	GKE cluster	configcheck-newsnapshot-tests	Error	Traffic from c blocked by ingres instance
High	cluster-3	GKE cluster	configcheck-newsnapshot-tests	Error	Traffic to publ by egress firewall
High	mysql-2	SQL instance	configcheck-newsnapshot-tests	Error	Connectivity i issue
High	mysql-1	SQL instance	configcheck-newsnapshot-tests	Error	Connectivity i
Medium	dynamic-routes-peer	Network	configcheck-newsnapshot-tests	Error	Dynamic route a peering static r
Medium	dynamic-routes-peer	Network	configcheck-newsnapshot-tests	Error	Dynamic route a subnet route

Network insight	Node to control plane connectivity is blocked by a routing issue or missing network peering
Priority	High
Insight type	Error
GKE cluster	cluster-2
Control plane endpoint	10.17.0.2
Network	gke
Project	configcheck-newsnapshot-tests
First report time	Apr 20, 11:00 PM
Documentation	View related product documentation

DISMISS INSIGHT

Let’s ask Gemini

How can I find out the average latency between my VMs in us-east4 and us-central1?

To find out the average latency between your VMs in us-east4 and us-central1, you can use the Performance Dashboard.

The Performance Dashboard shows latency metrics between VMs across all Google Cloud regions and internet endpoints.

*Gemini responses may vary

Today's agenda

01 Monitoring — real time

02 Lab: Resource Monitoring ✓ IoC

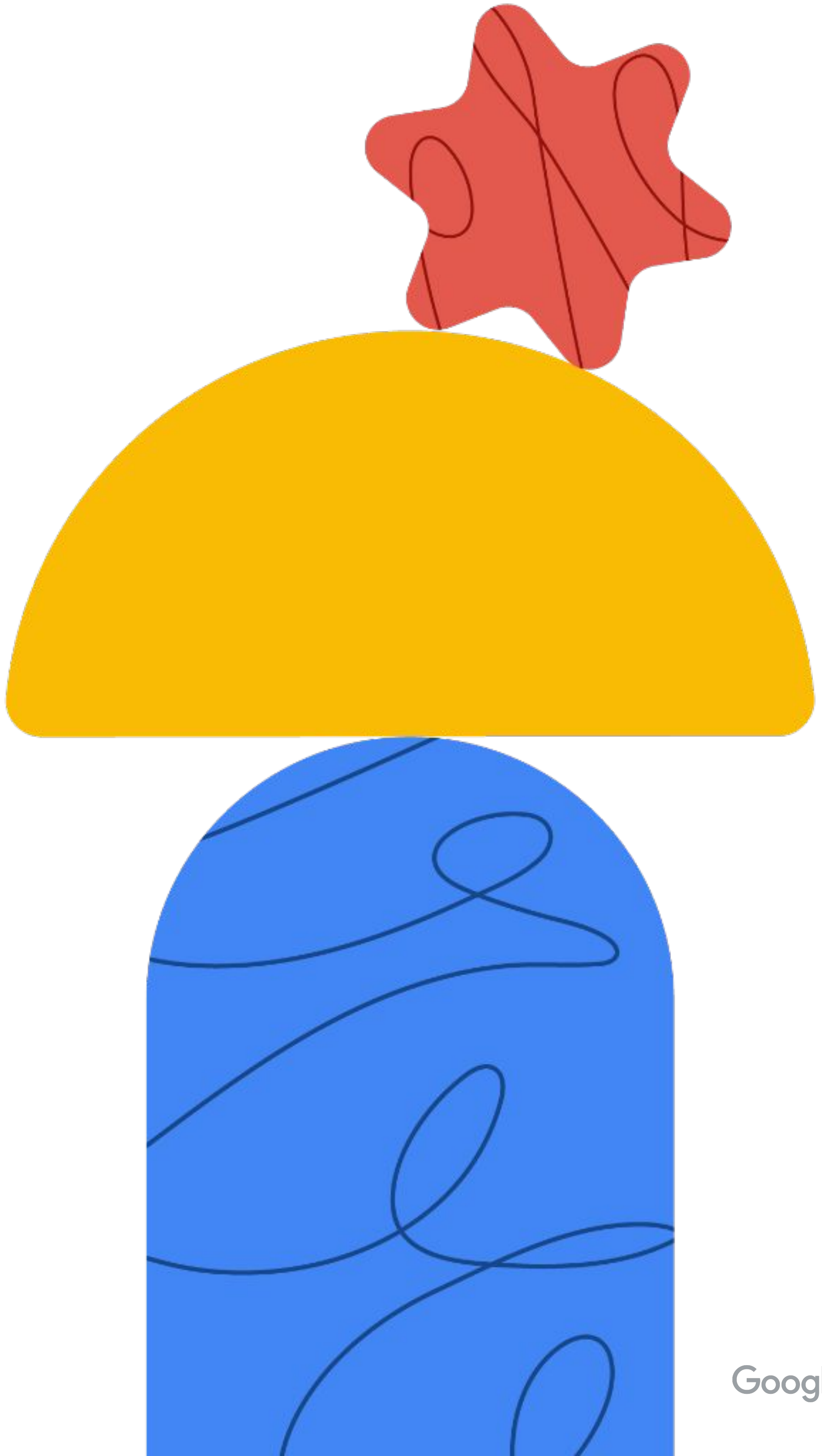
03 Logging — past — SIEM

04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

Lab intro

Resource Monitoring



Today’s agenda

01 Monitoring

02 Lab: Resource Monitoring

03 Logging

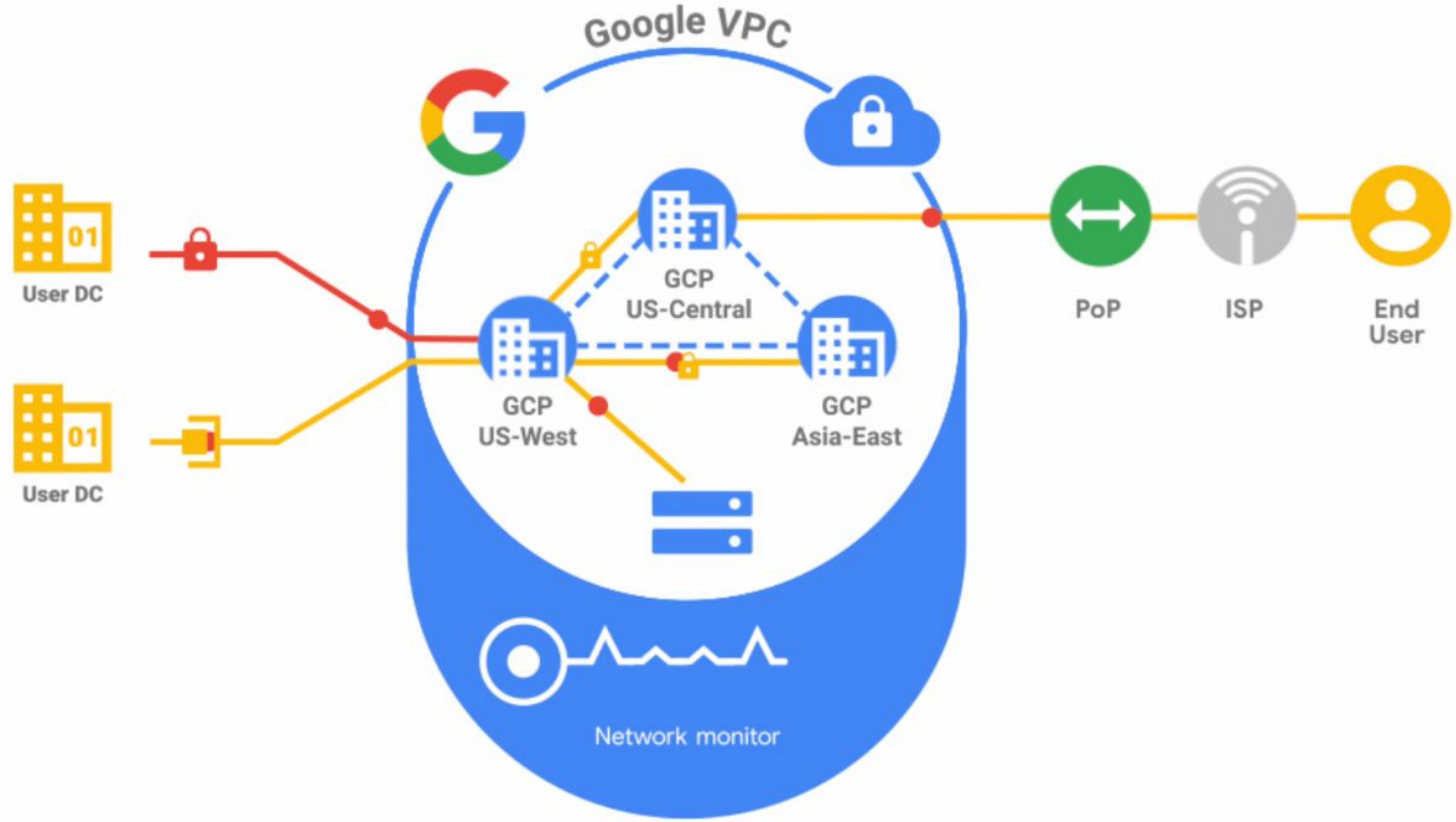
04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

fabric – zero impact

no payload

VPC Flow Logs record a sample of network flows



Enable VPC Flow Logs per VPC subnet

5 tuple

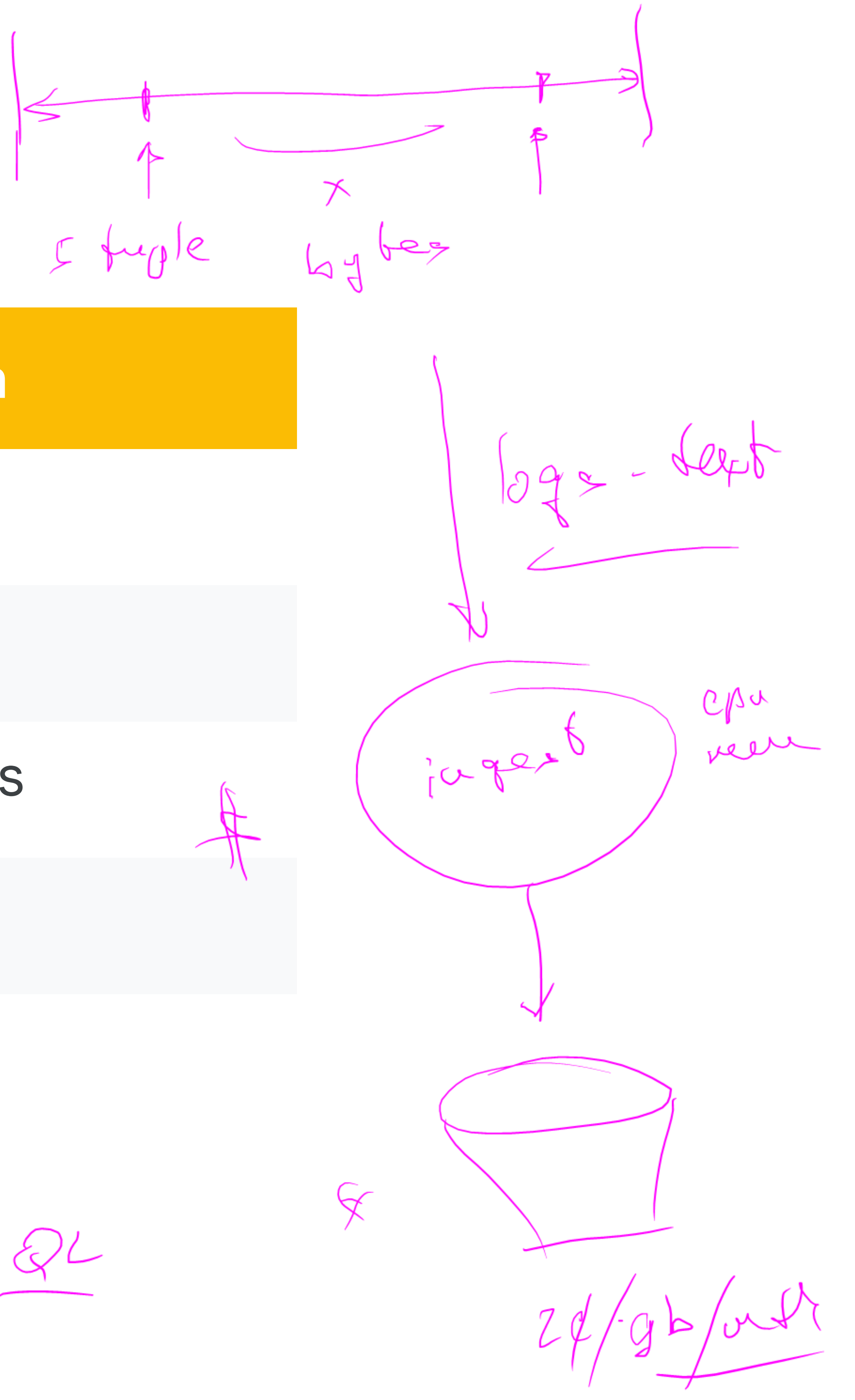
table schema

Field	Type	Description
src_ip	string	Source IP address
src_port	int32	Source port
dest_ip	string	Destination IP address
dest_port	int32	Destination port

protocol

export

BigQuery - SQL



Example of VPC Flow Logs

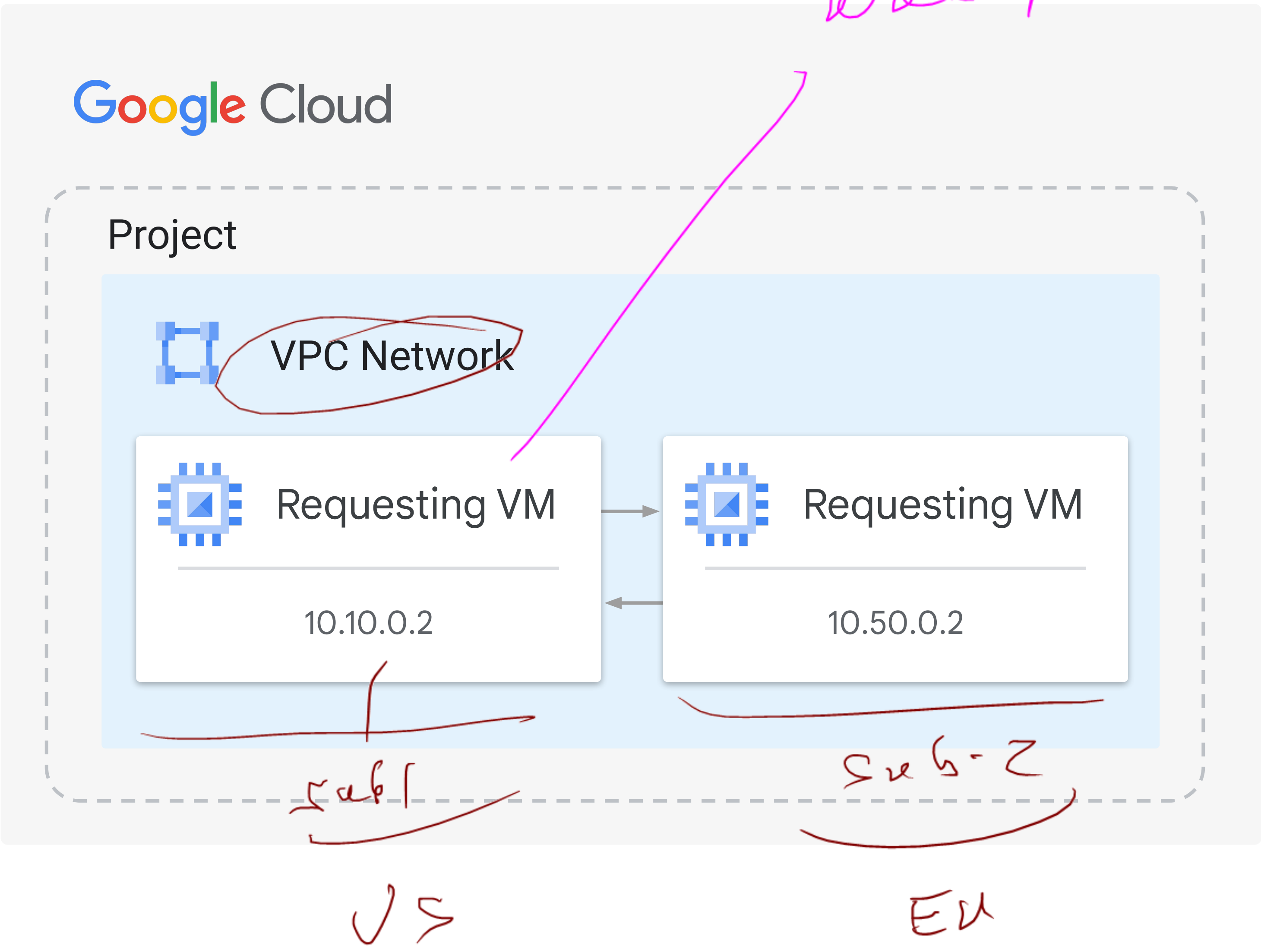
Subnet

see — block egress) for
* not see — block ingress

traffic
what VM sees

As reported by requesting VM (10.10.0.2)

request/reply	request	reply
connection.src_ip	10.10.0.2	10.50.0.2
connection.dest_ip	10.50.0.2	10.10.0.2
bytes_sent	1224	5342

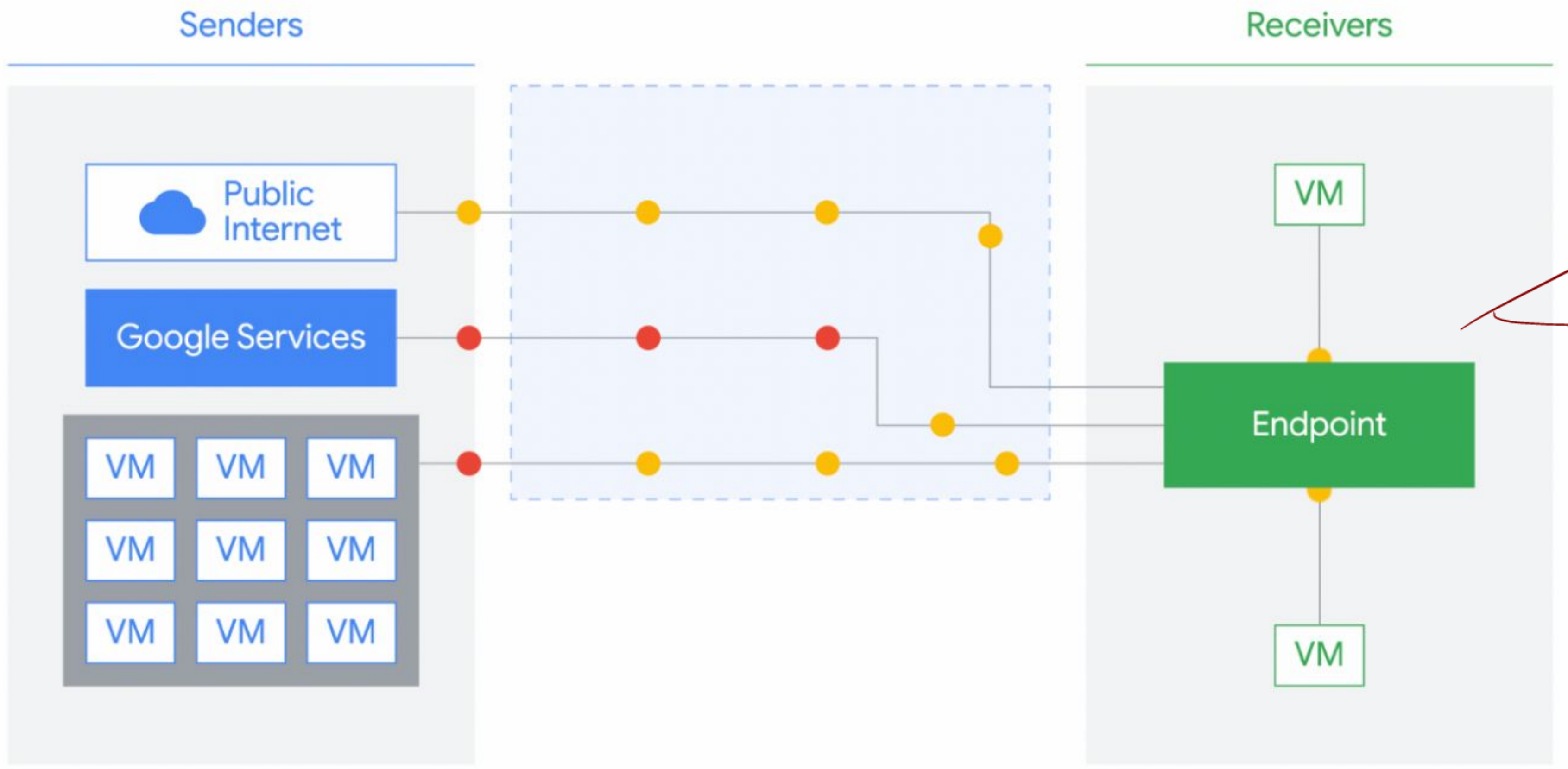


impact on VPC

Packet Mirroring clones the traffic of specified instances in your VPC network

Payload

mirror



security SIEM / IDS

wireshark

Cloud NAT logging allows you to log NAT connections and errors

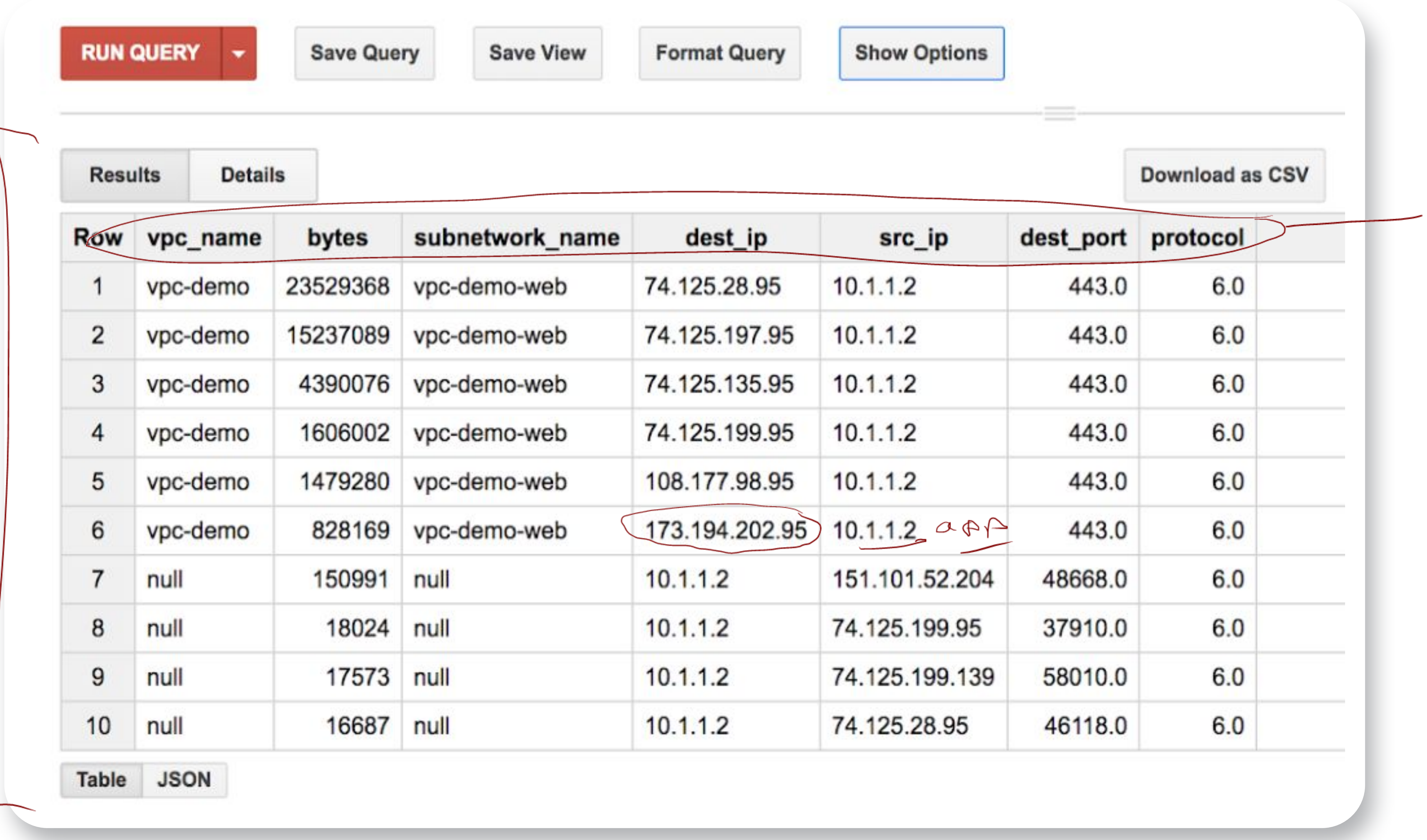
Logs are generated for the following scenarios:

- ✓ When a network connection using NAT is created.
- ✓ When a packet is dropped because no port was available for NAT. ← PAT

SQL

Analyze logs in BigQuery and visualize in Looker Studio

charts/graphs



schema ✓

Row	vpc_name	bytes	subnetwork_name	dest_ip	src_ip	dest_port	protocol
1	vpc-demo	23529368	vpc-demo-web	74.125.28.95	10.1.1.2	443.0	6.0
2	vpc-demo	15237089	vpc-demo-web	74.125.197.95	10.1.1.2	443.0	6.0
3	vpc-demo	4390076	vpc-demo-web	74.125.135.95	10.1.1.2	443.0	6.0
4	vpc-demo	1606002	vpc-demo-web	74.125.199.95	10.1.1.2	443.0	6.0
5	vpc-demo	1479280	vpc-demo-web	108.177.98.95	10.1.1.2	443.0	6.0
6	vpc-demo	828169	vpc-demo-web	173.194.202.95	10.1.1.2 app	443.0	6.0
7	null	150991	null	10.1.1.2	151.101.52.204	48668.0	6.0
8	null	18024	null	10.1.1.2	74.125.199.95	37910.0	6.0
9	null	17573	null	10.1.1.2	74.125.199.139	58010.0	6.0
10	null	16687	null	10.1.1.2	74.125.28.95	46118.0	6.0

Today's agenda

01 Monitoring

02 Lab: Resource Monitoring

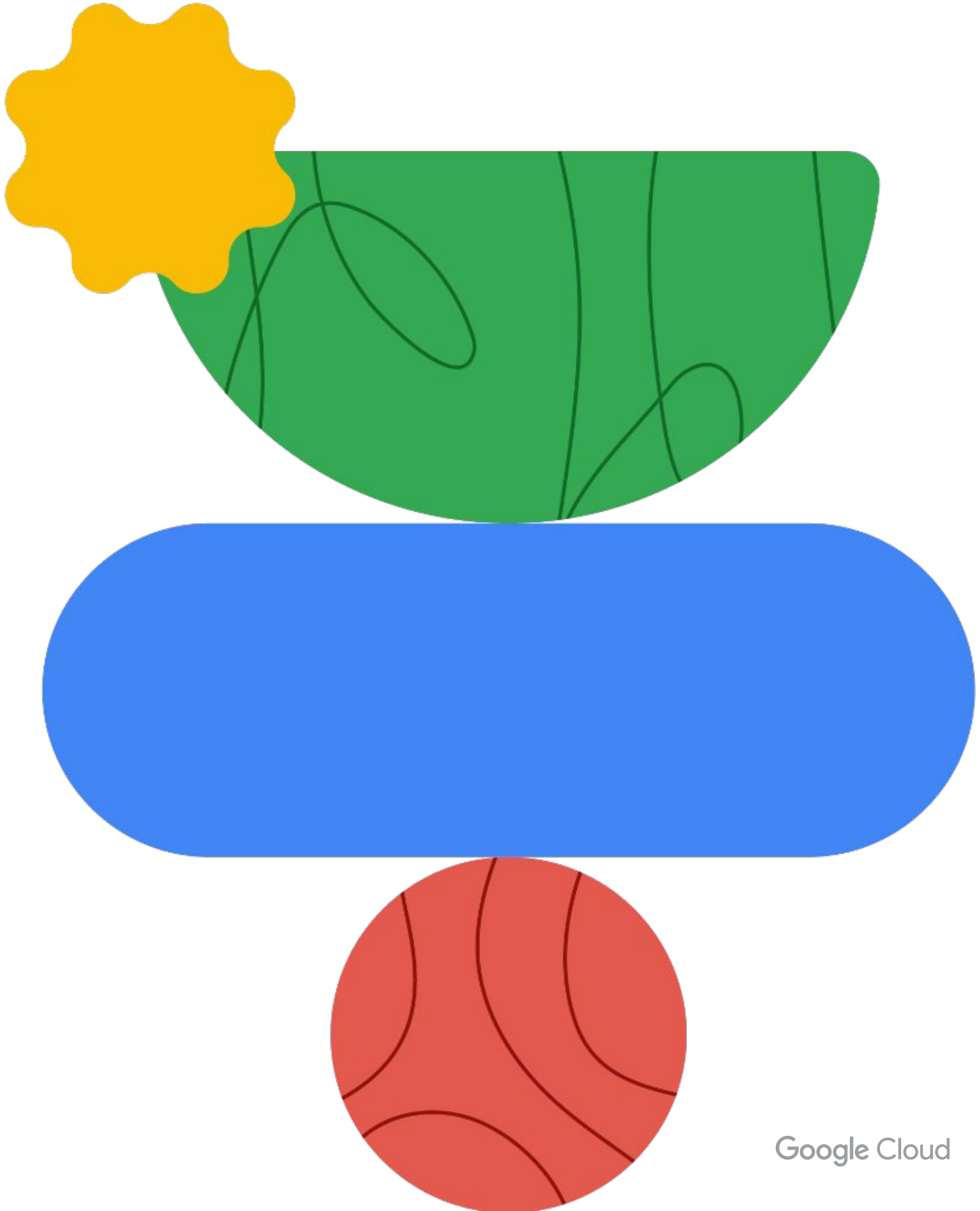
03 Logging

04 **Lab: Analyzing Network Traffic with VPC Flow Logs**

05 Quiz

Lab intro

Analyzing Network Traffic with
VPC Flow Logs



Today's agenda

01 Monitoring

02 Lab: Resource Monitoring

03 Logging

04 Lab: Analyzing Network Traffic with VPC Flow Logs

05 Quiz

Quiz | Question 1

Question

Which of the following two Google Cloud Monitoring features will notify you through email, SMS, or other channels when your web server cannot be reached?

A. Dashboards

B. Alerting policies

C. Uptime checks

D. Ops Agent

Quiz | Question 1

Answer

Which of the following two Google Cloud Monitoring features will notify you through email, SMS, or other channels when your web server cannot be reached?

A. Dashboards

B. [✓ Alerting policies]

C. [✓ Uptime checks]

D. Ops Agent

Quiz | Question 2

Question

In regards to VPC Flow Logs, which of the following statements is correct?

A. There is a delay and performance penalty in routing logged IP packets.

B. Log updates are provided every 5 minutes.

C. Logs cannot be analyzed in BigQuery or visualized in Looker Studio.

D. Logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.

Quiz | Question 2

Answer

In regards to VPC Flow Logs, which of the following statements is correct?

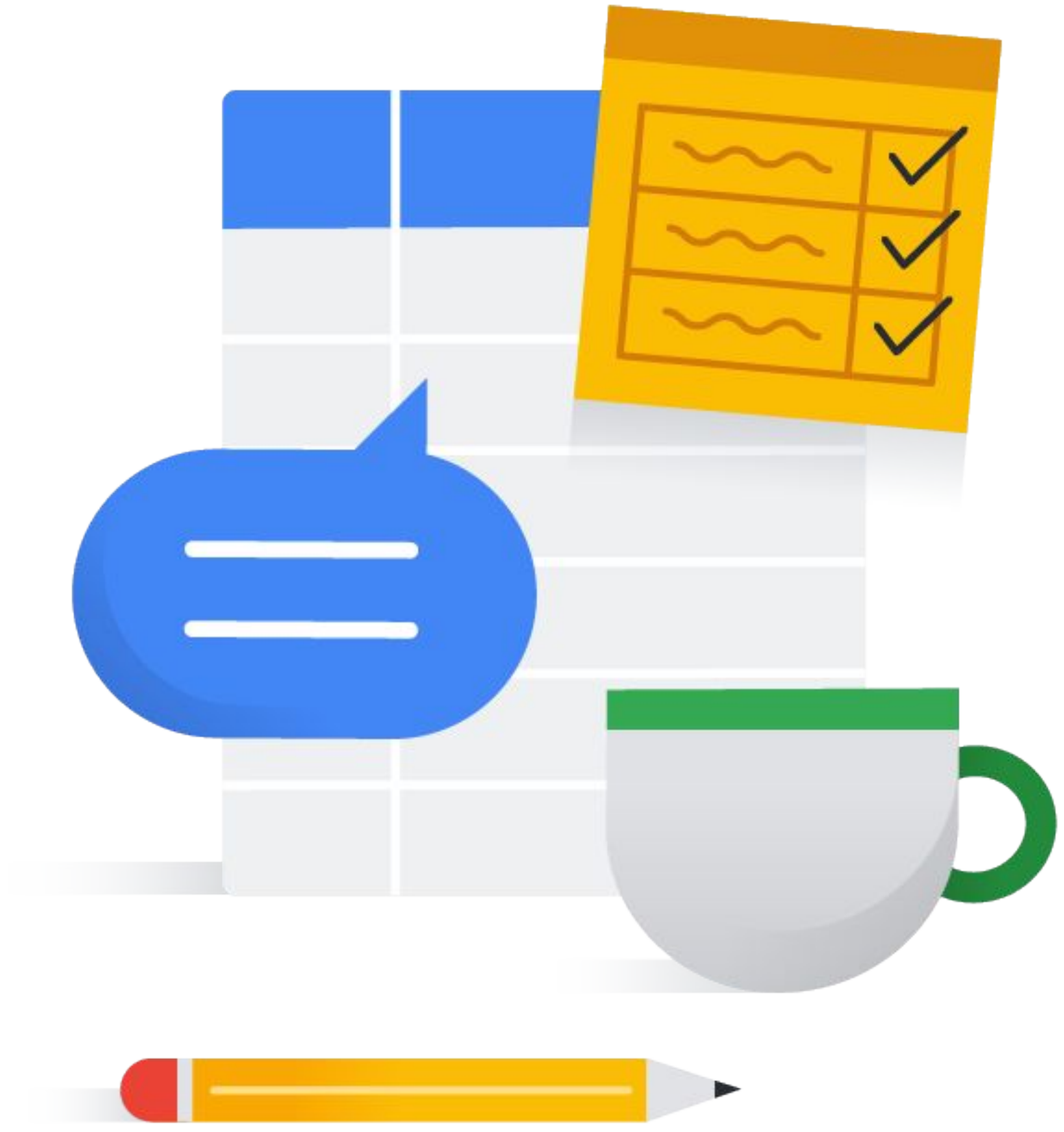
A. There is a delay and performance penalty in routing logged IP packets.

B. Log updates are provided every 5 minutes

C. Logs cannot be analyzed in BigQuery or visualized in Looker Studio

D. Logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization ✓

Debrief



Thank you.