



BLUE
TEAM
→ SECURITY INCIDENT RESPONSE

Incident Response
Google Cloud Platform

```
(dvirus@gondor)-[~]  
└─$ whoami
```



Daniel Rodriguez

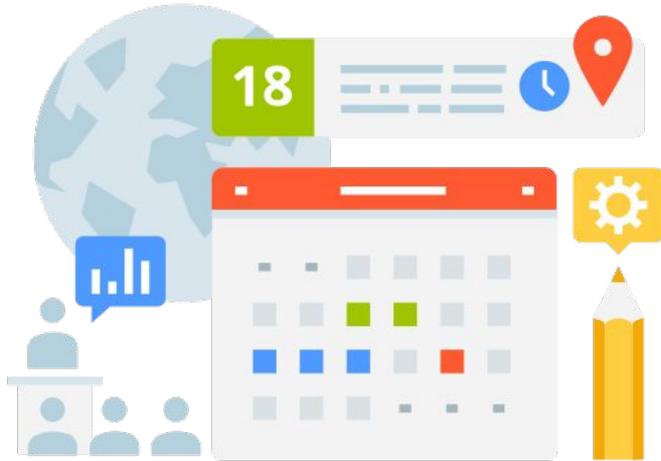
Security Consultant

Incident Response / Digital Forensics

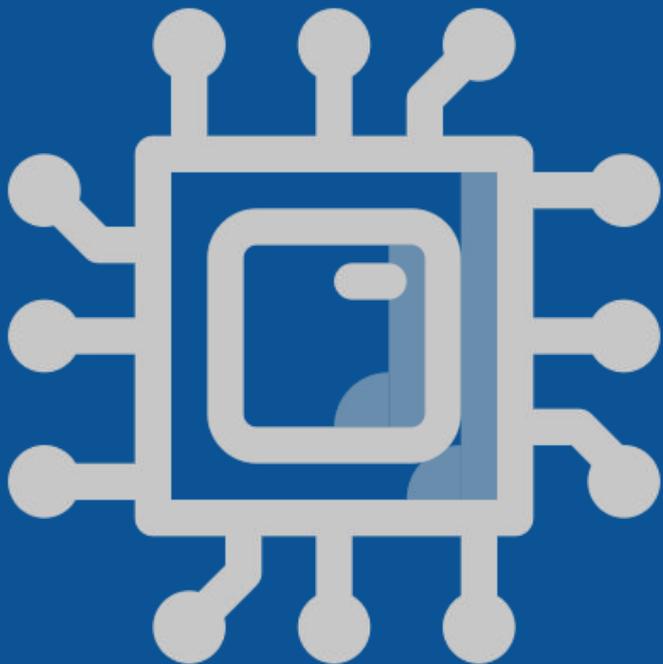
Twitter @dvirus

Website: <https://dvirus.training/>

Agenda



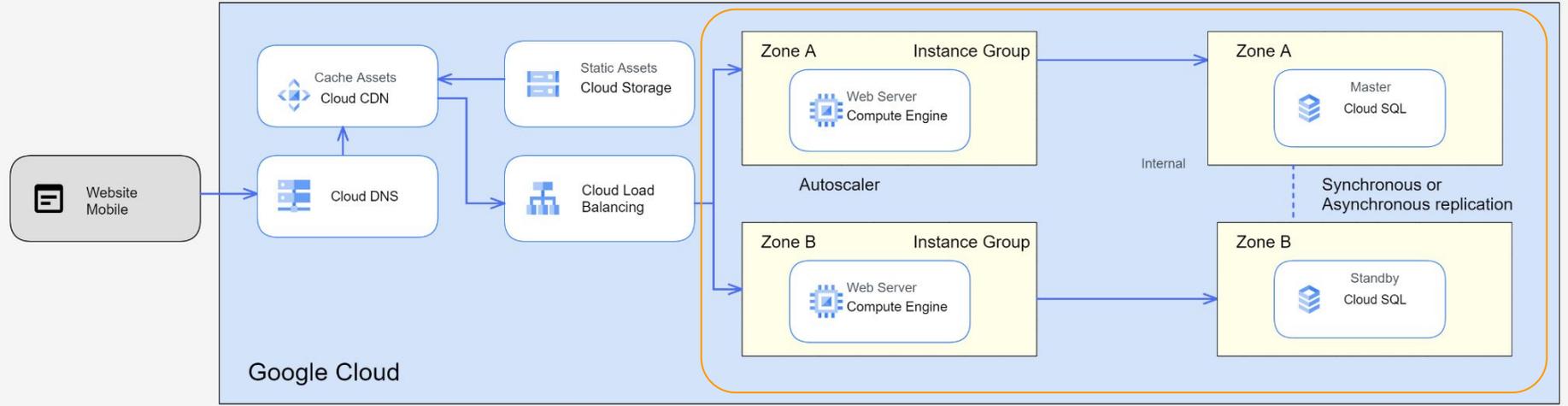
- Investigation of VMs Attacks
- VM logs
- Network Logs
- Network Traffic
- Snapshots
- Questions
- 🍕 + 🍺



Investigating VM Attacks

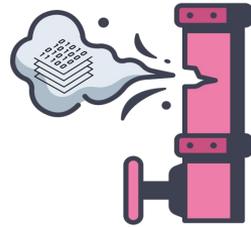
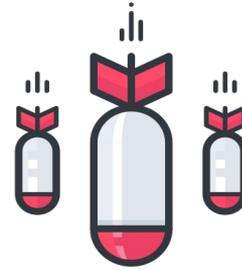
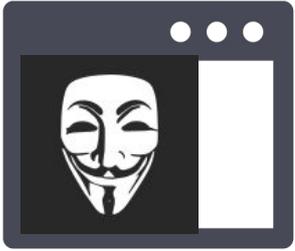
Architecture

Application on Virtual Machines in Google Cloud

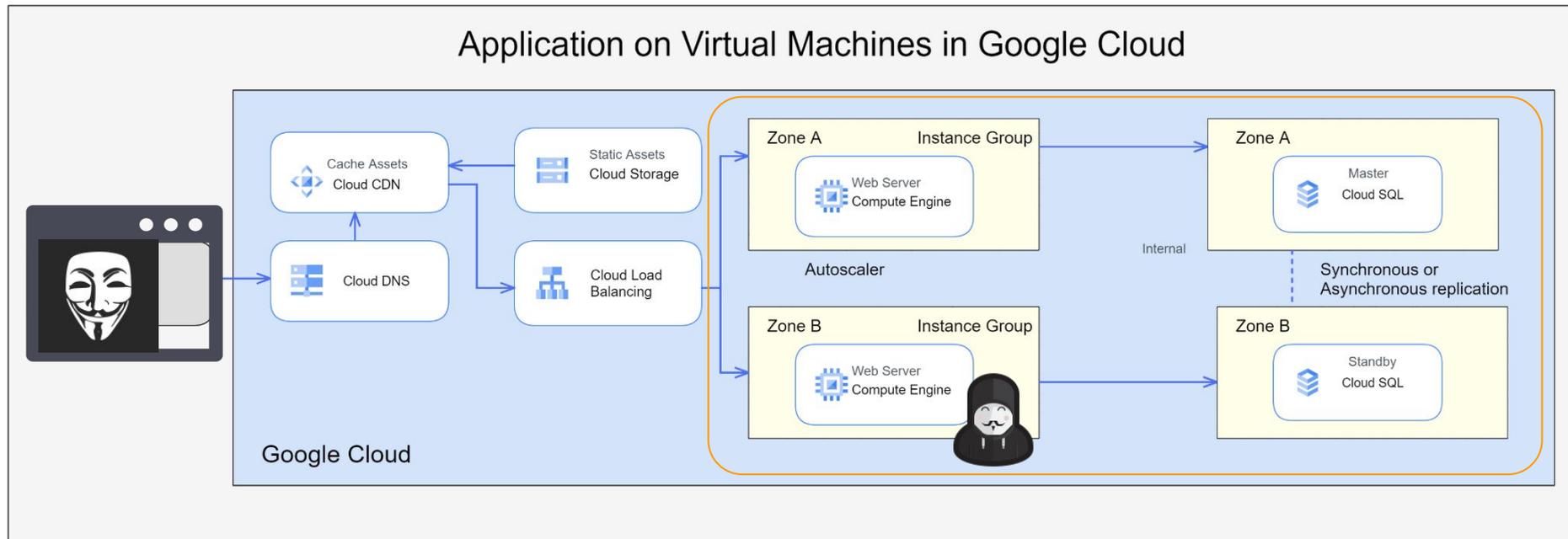


 VPC

VMs Impacts



The Incident | Defacement in GCP



 VPC

The Incident | Playbooks

PLAYBOOK - UNAUTHORIZED ACCESS

The unauthorized access incident response playbook contains all 7 steps defined by the NIST incident response process: Prepare, Detect, Analyze, Contain, Eradicate, Recover, Post-Incident Handling.

Prepare
Detect
Analyze
Contain
Eradicate
Recover
Post-Incident Handling

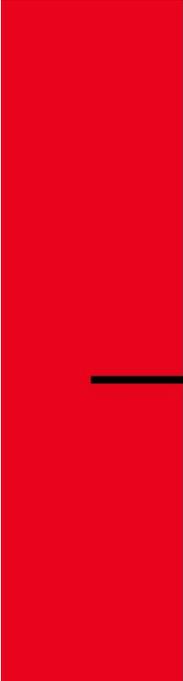
In the future, you will be able to create your own playbooks and share them with your colleagues and the Incident Response community here at [IncidentResponse.org](https://www.incidentresponse.org).

DOWNLOAD PLAYBOOK - PDF

DOWNLOAD PLAYBOOK - VISIO



<https://www.incidentresponse.org/playbooks/>



INCIDENT RESPONSE METHODOLOGY
IRM #6
WEBSITE
DEFACEMENT

Live reaction on a compromised web server

IRM Author: CERT SG
Contributor: CERT aDvens
IRM version: 2.0
E-Mail: cert.sg@socgen.com
Web: <https://cert.societegenerale.com>
Twitter: @CertSG

C'EST VOUS L'AVENIR SOCIETE GENERALE

<https://github.com/certsocietegenerale/IRM>

Logs access control



Attack Trees



Attack Flow

<https://center-for-threat-informed-defense.github.io/attack-flow/>

Attack Flow is a language for describing how adversaries combine and sequence various offensive techniques to achieve their goals. The project helps defenders and leaders understand how adversaries operate and improve their own defensive posture.

Investigation - Sources of evidence



Access Logs (VM)
/var/log/nginx/access.log



VPC Firewall Logs
Disabled by default



VPC Flow Logs
Disabled by default

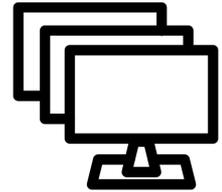
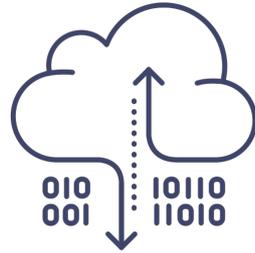


Packet Capture
Disabled by default



VM Forensic Image

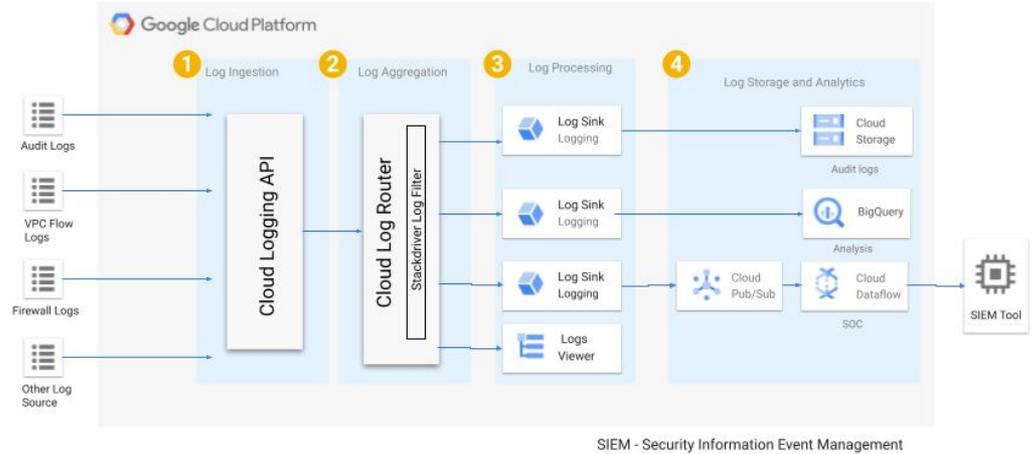
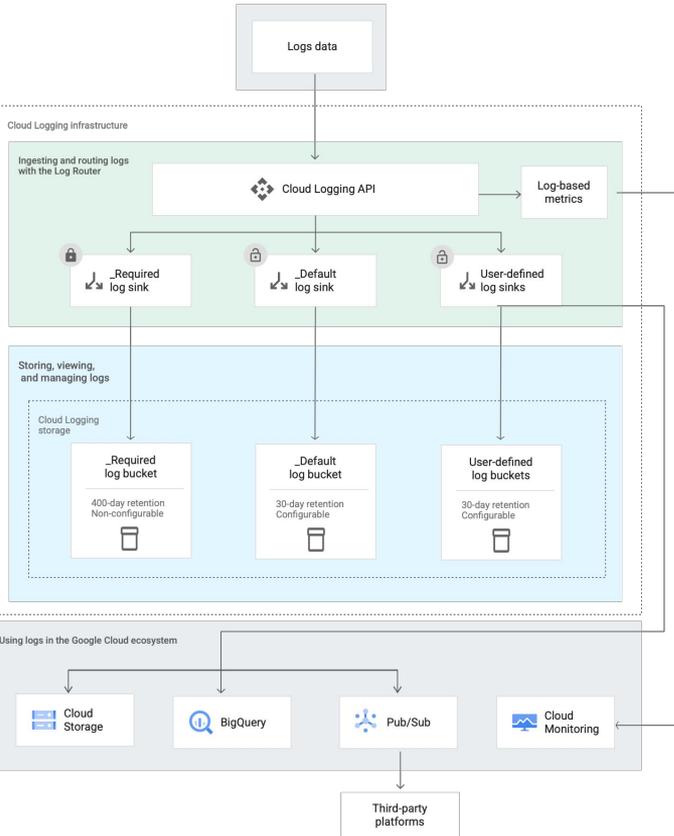
Pricing





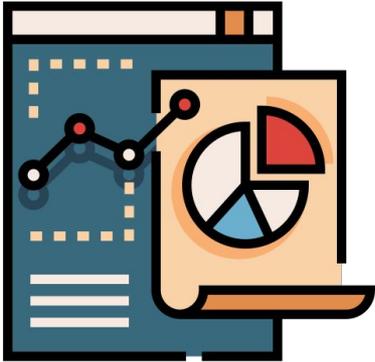
Investigating VM Logs

Google Cloud Logging



<https://cloud.google.com/logging/docs/reference/v2/rest/#service:-logging.googleapis.com>

Google Cloud Ops Agent



The Ops Agent is the primary agent for collecting telemetry from your Compute Engine instances. Combining logging and metrics into a single agent, the Ops Agent uses Fluent Bit

Linux: Syslog

Windows: EVTX logs

<https://cloud.google.com/stackdriver/docs/solutions/agents/ops-agent>

Google Cloud Ops Agent

Download

```
curl -sSO https://dl.google.com/cloudagents/add-google-cloud-ops-agent-repo.sh
```

Install

```
sudo bash add-google-cloud-ops-agent-repo.sh --also-install
```

Configuration File

```
vim /etc/google-cloud-ops-agent/config.yaml
```

Service Restart

```
sudo systemctl restart google-cloud-ops-agent"*"
```

Google Cloud Ops Agent

VM Details RESET ZOOM 1 HOUR ▾ MANAGE VM SSH ▾ SEND FEEDBACK ✕

webservers

Installed agent ✔ Ops Agent 2.23.0

Integrations (2) ✔ Host Metrics ✔ Linux Syslog

Alerts No open incidents →

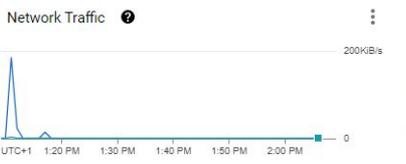
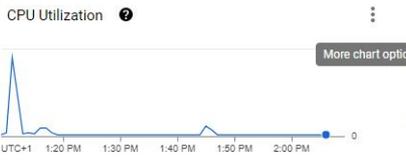
Events No recent events →

Uptime Checks No failed checks →

Additional details: instance_id : 7831651878476981217 zone : us-west1-b [View Details](#)

METRICS LOGS

- Overview
- CPU
- Processes
- Memory
- Network
 - Summary
 - Packet Mirroring
- Disk
 - Performance
 - Capacity



METRICS **LOGS**

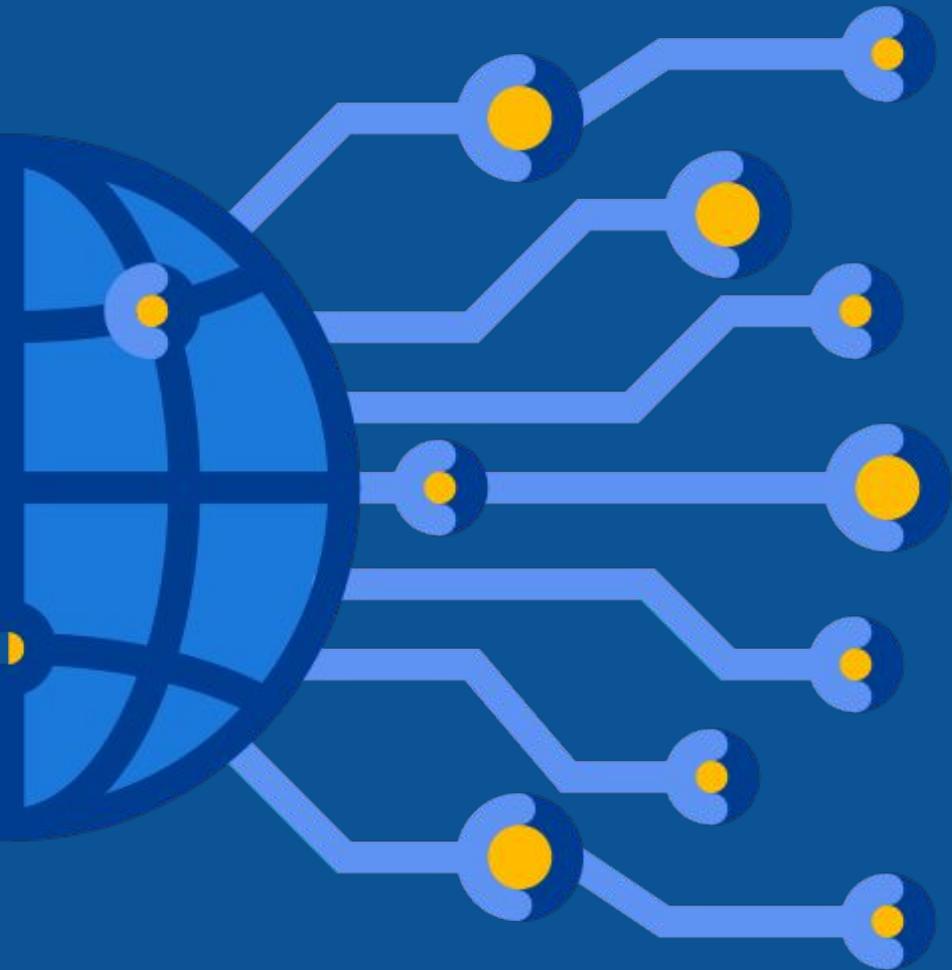
Logs 50 log entries Severity: Default Filter Search all fields and values

SEVERITY	TIMESTAMP	SUMMARY
★	2022-12-02 13:39:54.773 CET	Dec 2 12:39:54 debian dhclient[332]: bound to 10.138.0.3 -- renewal in 1738 seconds.
★	2022-12-02 13:42:49.165 CET	Dec 2 12:42:49 debian systemd[1]: Starting GCE Workload Certificate refresh...
★	2022-12-02 13:42:49.175 CET	Dec 2 12:42:49 debian gce_workload_cert_refresh[11630]: 2022/12/02 12:42:49: Error getting config status, workload certifica...
★	2022-12-02 13:42:49.175 CET	Dec 2 12:42:49 debian gce_workload_cert_refresh[11630]: 2022/12/02 12:42:49: Done
★	2022-12-02 13:42:49.178 CET	Dec 2 12:42:49 debian systemd[1]: gce-workload-cert-refresh.service: Succeeded.
★	2022-12-02 13:42:49.178 CET	Dec 2 12:42:49 debian systemd[1]: Finished GCE Workload Certificate refresh.
★	2022-12-02 13:51:05.438 CET	45.79.172.21 - - [02/Dec/2022:12:51:05 +0000] "\x16\x03\x01\x00\x85\x01\x00\x00\x01\x03\x03E\xDF\xD6\xE2W96\xB1Z\xDC\xB1\x17\xAD\xA8\x8E\xBBj\t\xDE\xBC\xF3sL\x8A\xA9P\x8C)\x0C/\x0B0\xC0+\x0B,\x0C\xA8\x0C\xA9\xC0\x13\xC0\x09\xC0\x14\x0C" 400 157 "-" "-"

▼ {
 insertId: "efj214f2a5bv5"
 jsonPayload: {
 message:
 "45.79.172.21 - - [02/Dec/2022:12:51:05 +0000]
 "\x16\x03\x01\x00\x85\x01\x00\x00\x01\x03\x03E\xDF\xD6\xE2W96\xB1Z\xDC\xB1\x17\xAD\xA8\x8E\xBBj\t\xDE\xBC\xF3sL\x8A\xA9P\x8C)\x0C/\x0B0\xC0+\x0B,\x0C\xA8\x0C\xA9\xC0\x13\xC0\x09\xC0\x14\x0C" 400 157 "-" "-"
 }
 }
}

[Open in Logs Explorer](#)





Investigating Network Logs

VPC Firewall Rules

 VPC network

 VPC networks

 IP addresses

 Bring your own IP

 **Firewall**

 Routes

 VPC network peering

 Shared VPC

 Serverless VPC access

 Packet mirroring

Firewall [+ CREATE FIREWALL POLICY](#) [+ CREATE FIREWALL RULE](#)

VPC firewall rules

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#).

 SMTP port 25 disallowed in this project 

[REFRESH](#) [CONFIGURE LOGS](#) [DELETE](#)

 **Filter** Enter property name or value

<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network 	Logs
<input type="checkbox"/>	allow-ingress-from-iap	Ingress	Apply to all	IP ranges: 35.23!	all	Allow	1000	default	Off
<input type="checkbox"/>	default-allow-http	Ingress	http-server	IP ranges: 0.0.0.(tcp:80	Allow	1000	default	Off
<input type="checkbox"/>	default-allow-https	Ingress	https-server	IP ranges: 0.0.0.(tcp:443	Allow	1000	default	Off

VPC Firewall Rules

VPC network

← Firewall rule details EDIT DELETE

VPC networks

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

default-allow-http

Description

Logs
Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

On
 Off

Additional fields ?

Include metadata

[^ HIDE LOGS DETAILS](#)

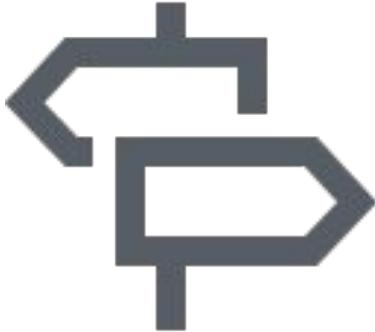
Network
default

Priority *
1000 [CHECK PRIORITY OF OTHER FIREWALL RULES](#) ?

Priority can be 0 - 65535

Direction
Ingress

VPC Flow Logs



VPC Flow Logs records a sample of network flows sent from and received by VM instances, including instances used as GKE nodes. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.

TCP and UDP / No ICMP

<https://cloud.google.com/vpc/docs/using-flow-logs>

VPC Flow Logs

VPC network

VPC networks

IP addresses

Bring your own IP

Firewall

Routes

VPC network peering

Shared VPC

Serverless VPC access

Packet mirroring

VPC network details

EDIT DELETE VPC NETWORK

Enable DNS API

Applying DNS server policies to the network requires DNS API. This is a one-time enablement per project and may take a few minutes to complete.

ENABLE API

None

Maximum transmission unit

1460

SUBNETS STATIC INTERNAL IP ADDRESSES FIREWALLS ROUTES VPC NETWORKS

ADD SUBNET FLOW LOGS

Filter Region: us-west Enter property name or value

Name	Region	Stack Type	Internal IP ranges	External IP ranges
<input checked="" type="checkbox"/> default	us-west1	IPv4	10.138.0.0/20	None
<input type="checkbox"/> default	us-west2	IPv4	10.168.0.0/20	None
<input type="checkbox"/> default	us-west3	IPv4	10.180.0.0/20	None
<input type="checkbox"/> default	us-west4	IPv4	10.182.0.0/20	None

VPC flow logs can increase costs

Turning on VPC flow logs won't affect performance, but some systems generate a large number of logs. This can increase costs in Cloud Logging as well as log export destinations such as BigQuery and Cloud Pub/Sub. [Learn more](#)

Manage these logs and resulting costs by adjusting the settings below, or in [Cloud Logging](#)

Aggregation Interval

5 SEC 30 SEC 1 MIN 5 MIN 10 MIN 15 MIN

Additional fields

Include metadata

Sample rate

50 %

Estimated logs generated per day: 465.63 KB

Depending on your traffic patterns, setting an aggregation interval of 30 sec can reduce your flow logs size by up to 83% compared to the default aggregation interval of 5s [Learn more](#)

CANCEL SAVE



VPC Flow Logs

Logs Explorer REFINE SCOPE Project

Query Recent (30) Saved (0) Suggested (1) Library

Last 1 hour Search all fields Resource

```
logName:(\"projects/velvety-broker-367220/logs/compute.googleapis.com%2Fvpc_flows\") AND resource.labels.subnetwork_id:(11525994588681926)
```

Log fields Histogram Create

Log fields <>

Search fields and values

RESOURCE TYPE

- Subnetwork 13

SEVERITY

- Default 13

Histogram

Query results 13 log entries Find in re

SEVERITY TIMESTAMP CET SUMMARY EDIT

Showing logs for last 1 hour from 12/2/22, 1:58 PM to 12/2/22, 2:58 PM. Extend time by: 1 hour Edit time

```
{\"bytes_sent\": \"3584\", \"connection\": {\"}, \"end_time\": \"2022-12-02T13:54:52.826044828Z\", \"packets_sent\": \"64\", \"src_vpc\": {\"}, \"start_time\": \"2022-12-02T13:54:47.706235314Z\"}
```

Hide log summary Expand nested fields

```
{  insertId: \"1fm783ff2uitgk\"  jsonPayload: {    bytes_sent: \"3584\"    connection: {3}    end_time: \"2022-12-02T13:54:52.826044828Z\"    packets_sent: \"64\"    reporter: \"SRC\"  }  src_instance: {    project_id: \"velvety-broker-367220\"    region: \"us-west1\"    vm_name: \"webservers\"    zone: \"us-west1-b\"  } }
```



Investigating Network Packets

Packet Mirroring



You can use Packet Mirroring to mirror traffic to and from particular virtual machine (VM) instances. The collected traffic can help you detect security threats and monitor application performance.

TCP/UDP load balancer is required

<https://cloud.google.com/vpc/docs/using-packet-mirroring>



Forensic Images

Snapshots



- Disk image of the current state of the VM
- Attach the snapshot to your DFIR instance
- Mount as a R/O

<https://cloud.google.com/compute/docs/disks/snapshots>

(dvirus@gondor)-[~]
\$ whoami



Daniel Rodriguez
Security Consultant
Incident Response / Digital Forensics
Twitter @dvirus
Website: <https://dvirus.training/>



FOOCAFE
Learn · Create · Share · Grow





Pizza Time