Fight the CRIME

BLUE TEAM

→ SECURITY INCIDENT RESPONSE

Incident Response

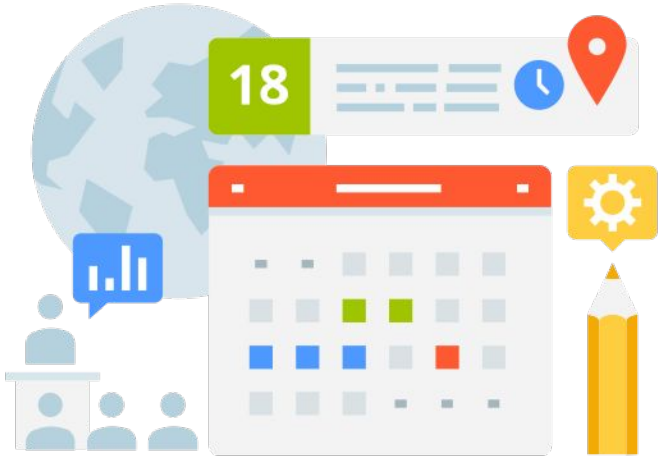
Google Cloud Platform

Hej

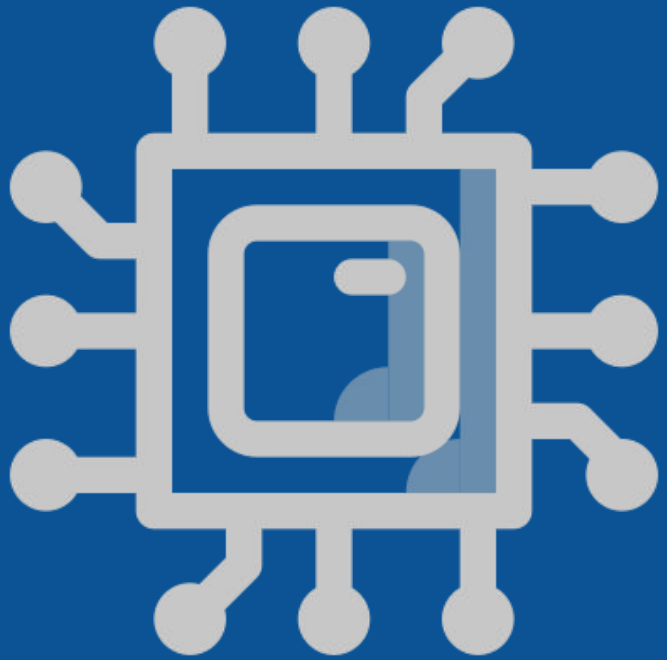
```
┌──(dvirus㉿gondor)-[~]
└─$ whoami
```

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

Agenda



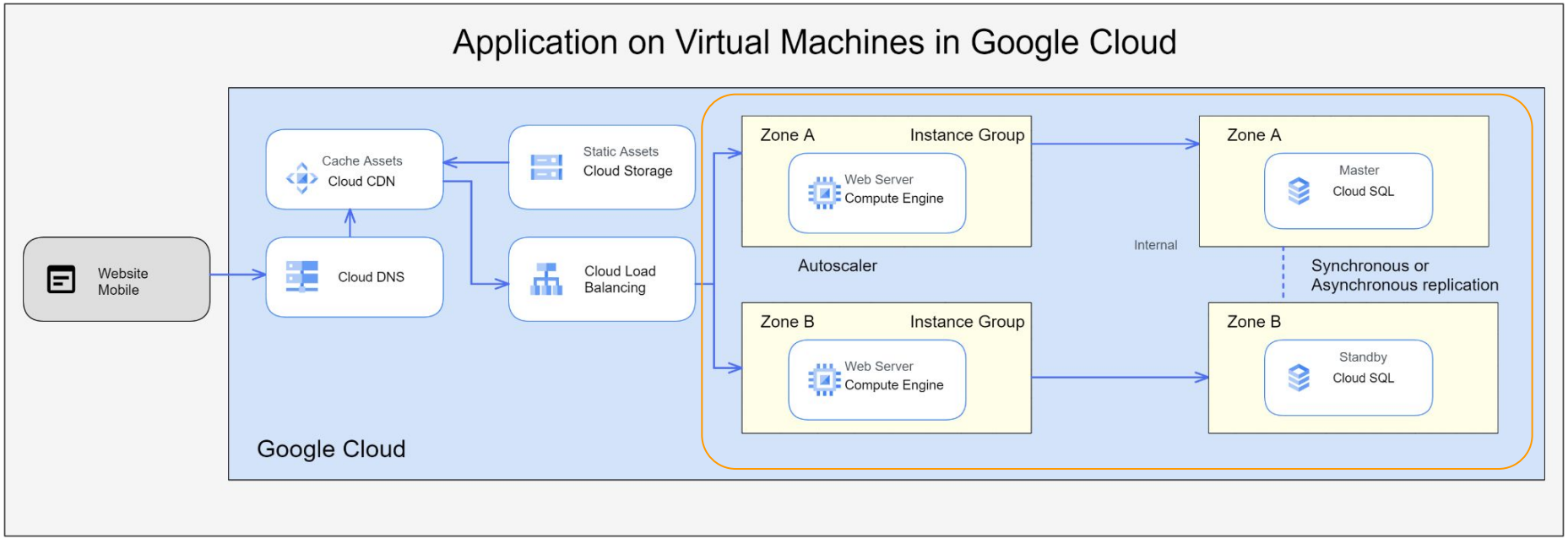
- Investigation of VMs Attacks
- VM logs
- Network Logs
- Network Traffic
- Snapshots
- Questions
- 



Investigating

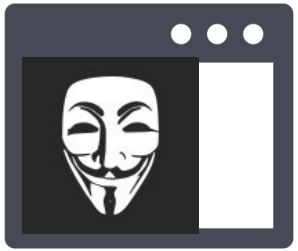
VM Attacks

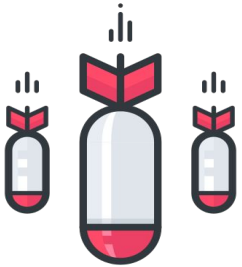
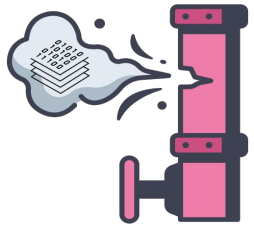
Architecture



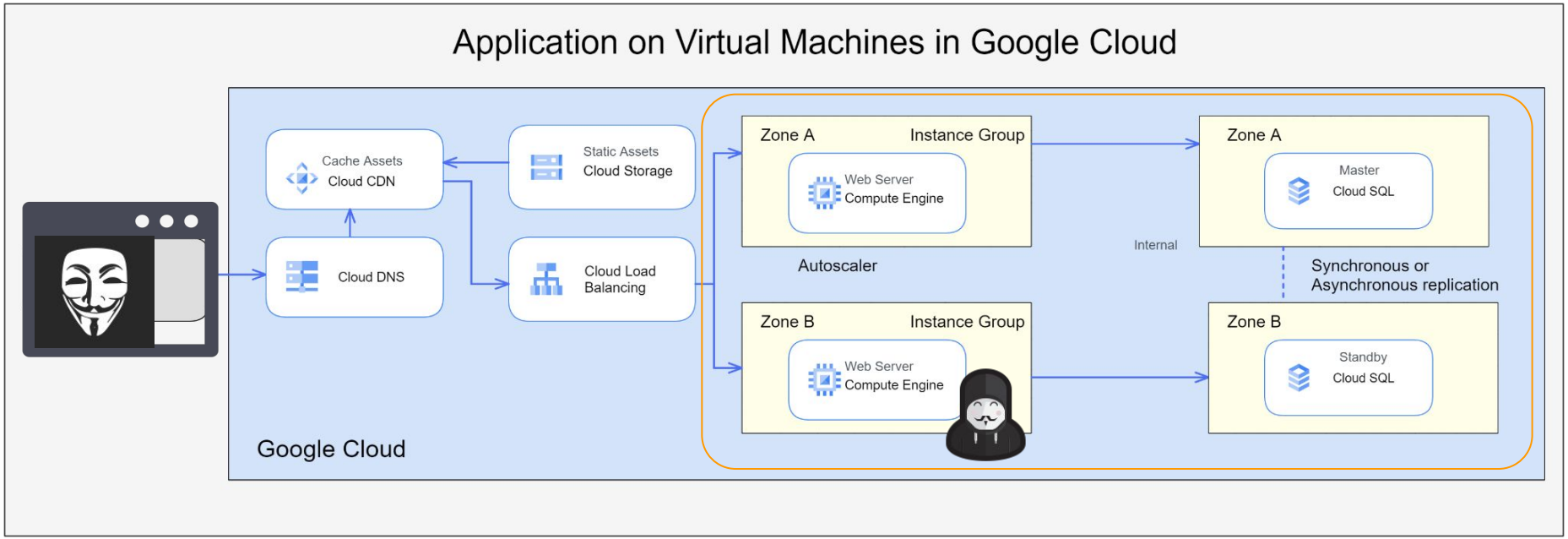
VPC

VMs Impacts



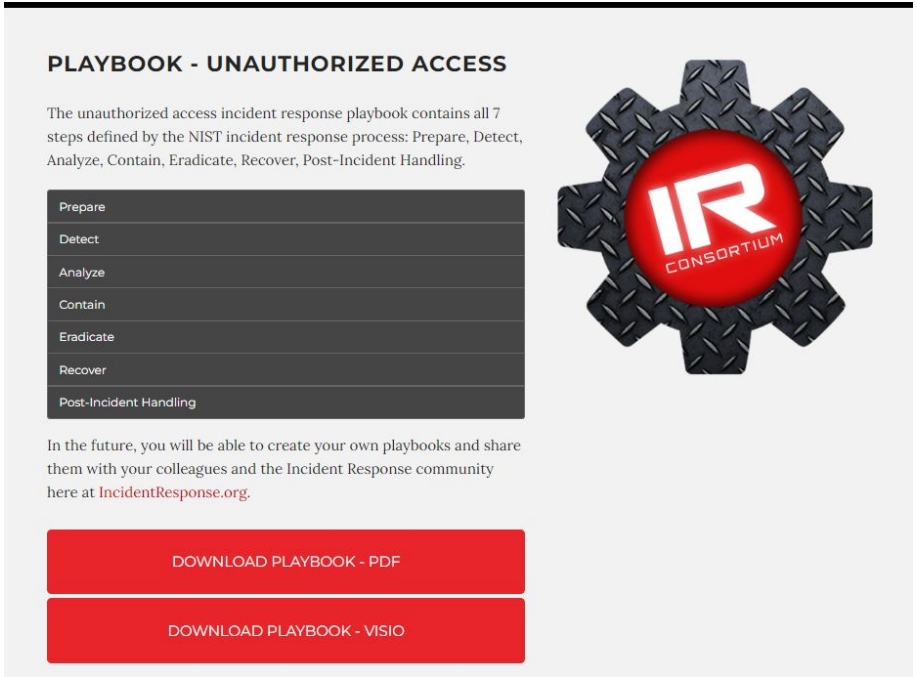




The Incident | Defacement in GCP



VPC

The Incident | Playbooks



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

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

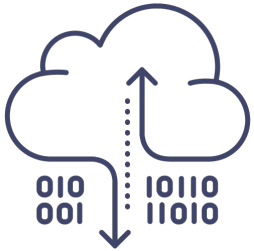
VPC Firewall Logs
Disabled by default

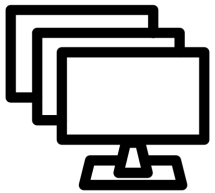
VPC Flow Logs
Disabled by default

Packet Capture
Disabled by default

VM Forensic Image

Pricing

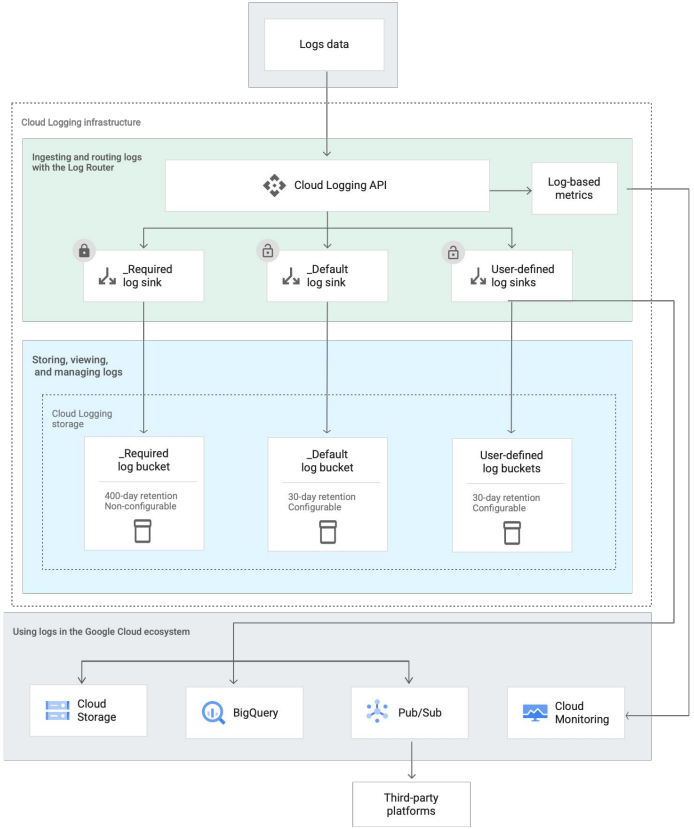


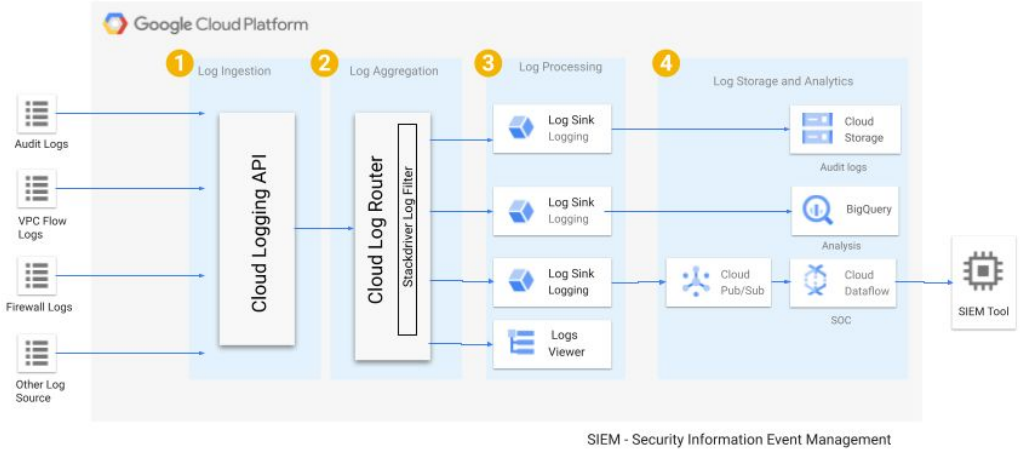


Investigating

VM Logs

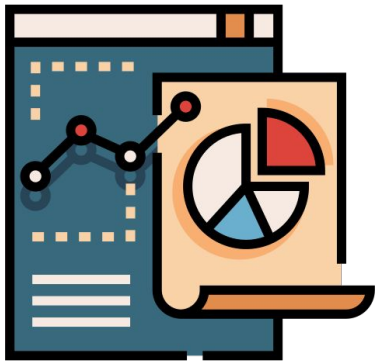
Google Cloud Logging





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
```

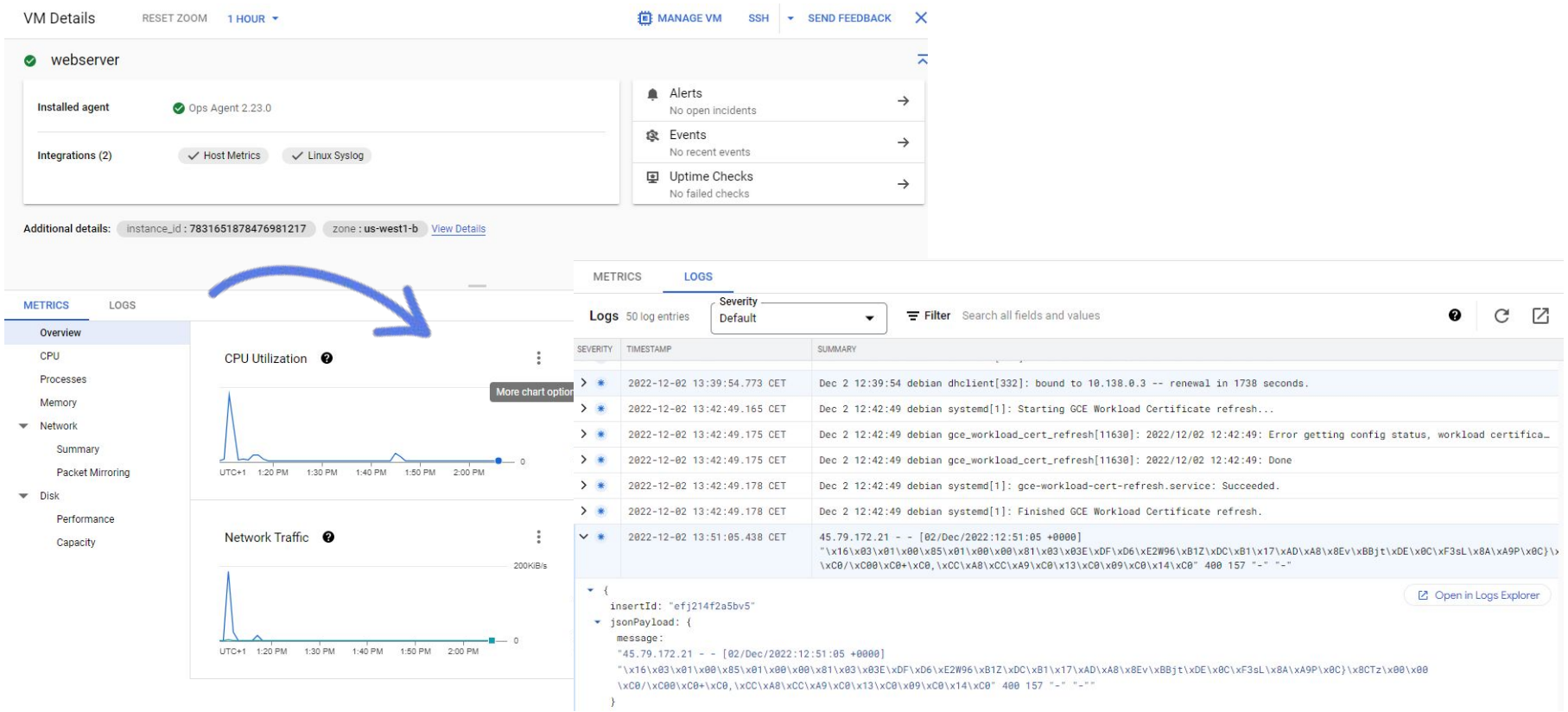
Configuration File

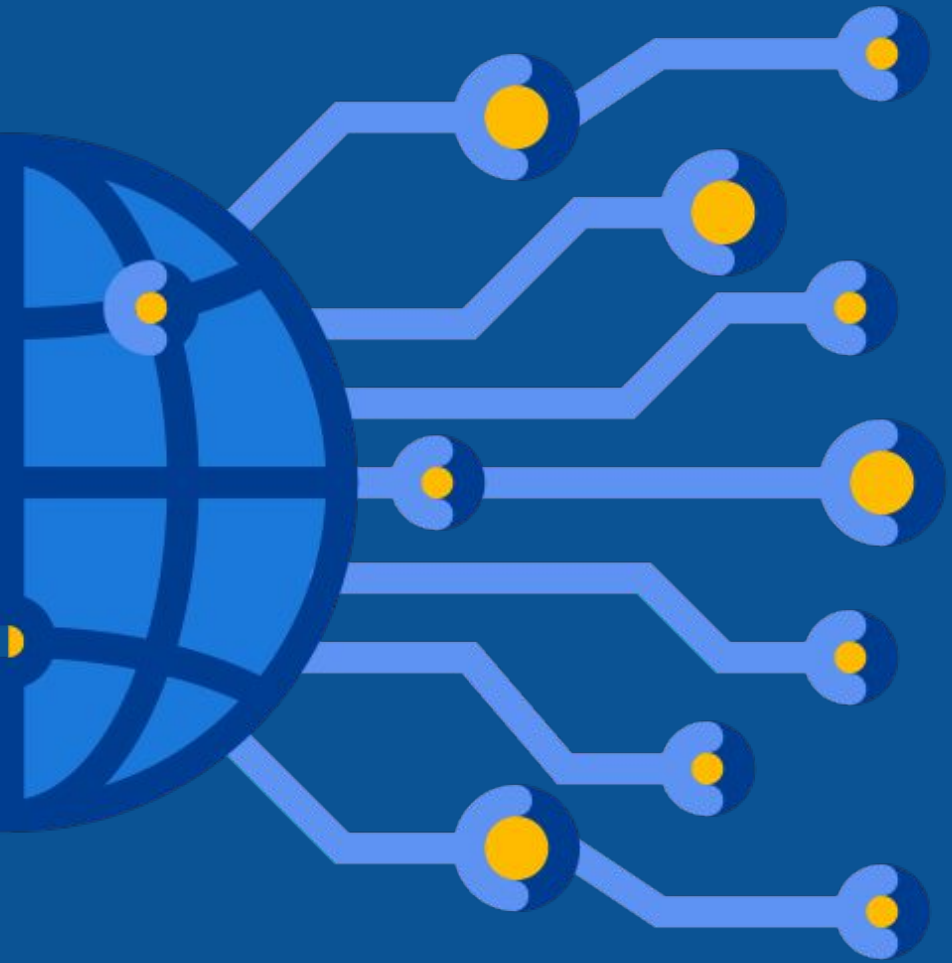
```
vim /etc/google-cloud-ops-agent/config.yaml
```

Service Restart

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

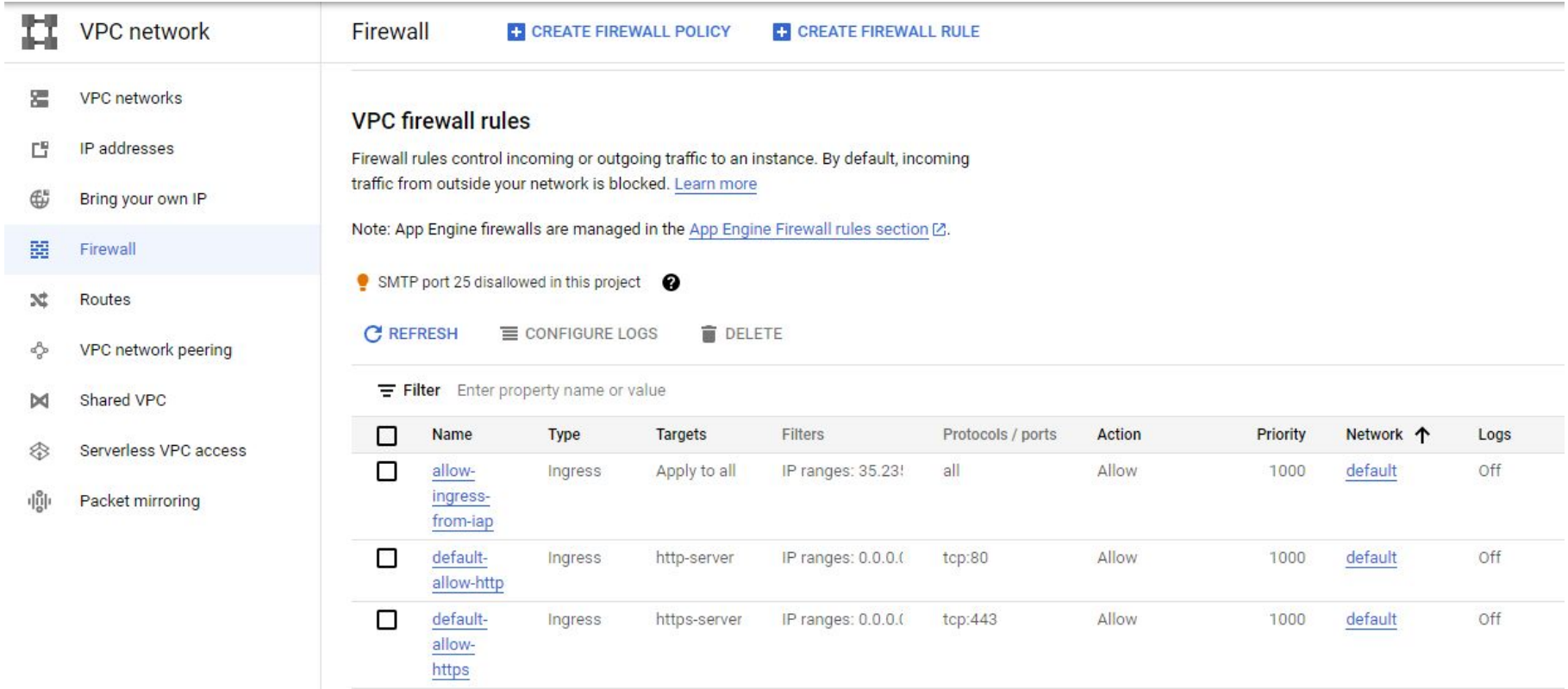
Google Cloud Ops Agent



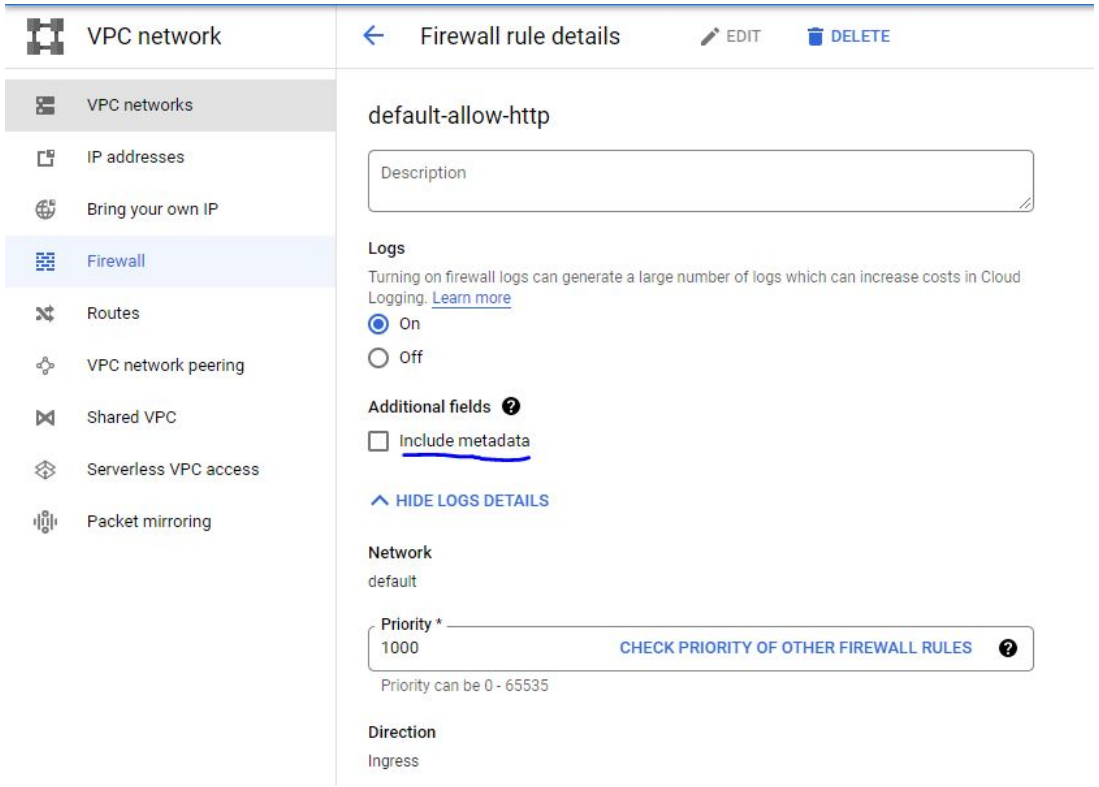


Investigating
Network Logs

VPC Firewall Rules



VPC Firewall Rules



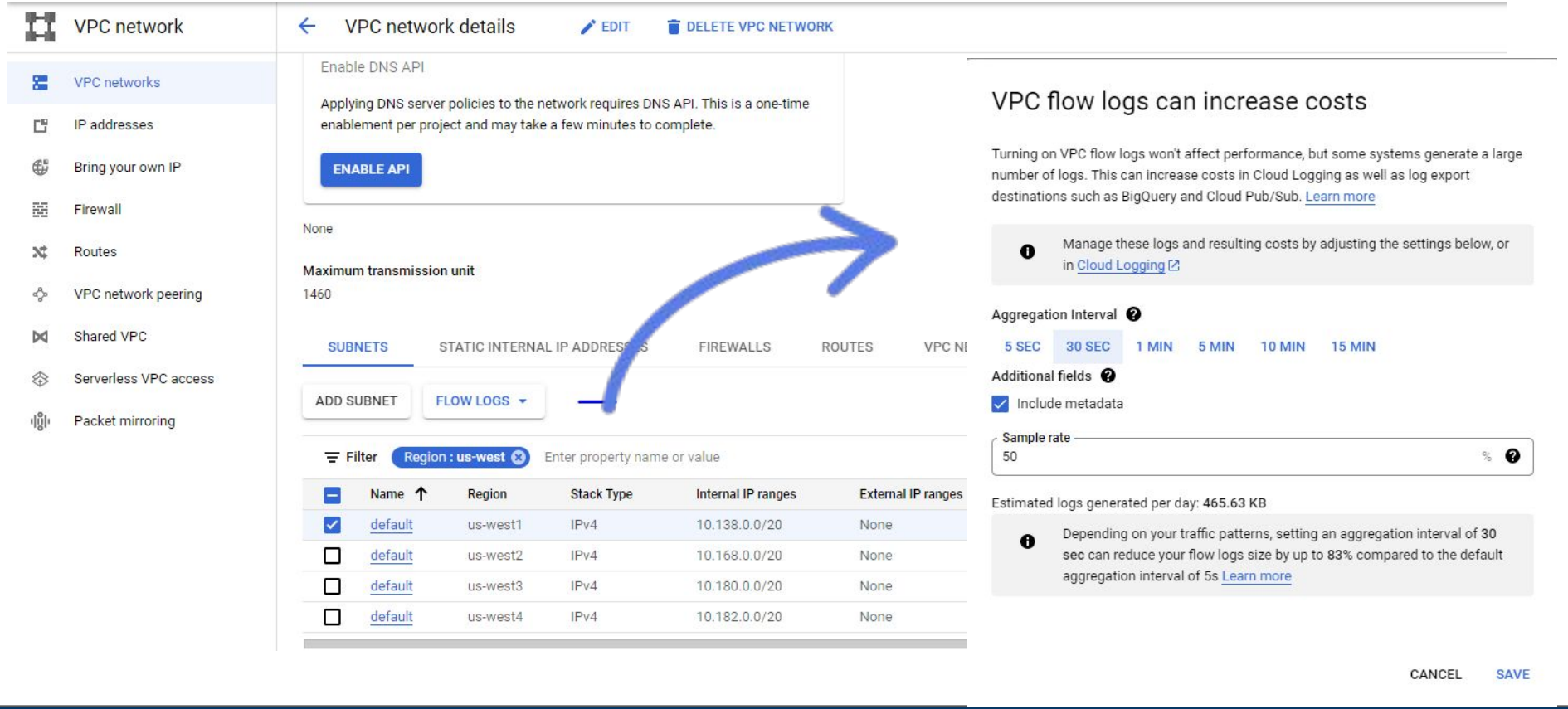
VPC Flow Logs

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.

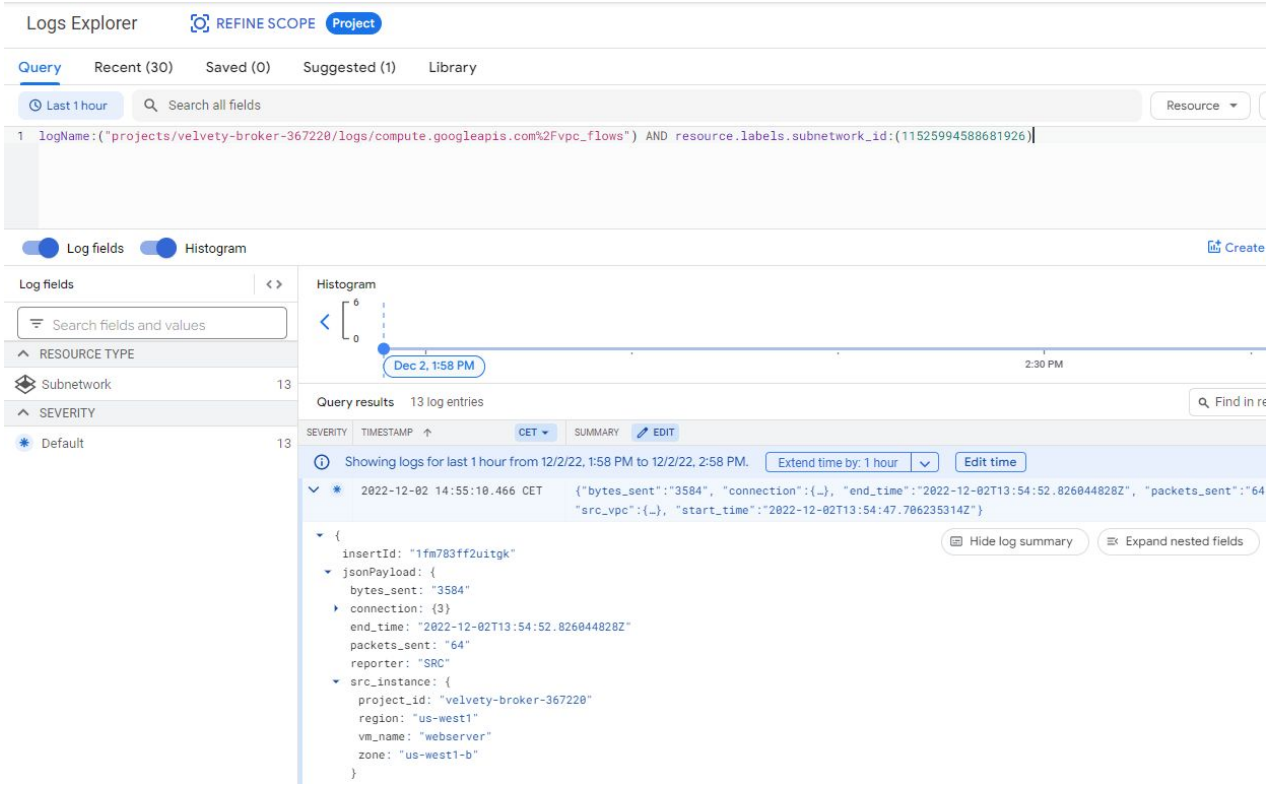
TCP and UDP / No ICMP

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

VPC Flow Logs



VPC Flow Logs



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/

Pizza Time