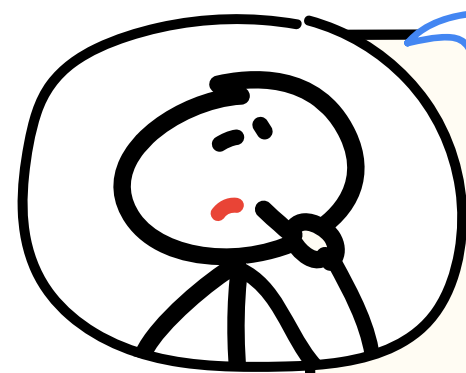




Cloud Armor

#GCPsketchnote

@PVERGADIA THECLOUDGIRL.DEV 10.29.2020



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

CLOUD ARMOR Policy P1

CLOUD ARMOR Policy P2

CLOUD ARMOR Policy P3

PROJECT web-frontend

backend-service-1

backend-service-2

backend-service-3

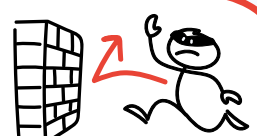
backend-service-4

ERIN

User traffic on our internet facing service is growing rapidly!

And so are the malicious attacks!

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



SAM



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 does Cloud Armor work?

CLOUD ARMOR: DDoS PROTECTION & WAF

Defense against L3/L4 volumetric and protocol DDoS attacks

HTTP(s)

Cloud CDN

HTTP(s) Load Balancing

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

Internet

Cloud Provider / Customer Datacenter

GKE Cluster

App Instance

Autoscaling



External Application

Hybrid or Multi Cloud Workload

L3/L4 Volumetric DDoS Protection

- DNS Amplification !
- SYN Flood X
- ICMP Flood !
- Slowloris X

Geography Based Access Controls

- origin: US ✓
- origin: UK X
- origin: SG ✓

Layer 7 Traffic Filtering & WAF

Google Cloud

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

Cloud Armor

Cloud Load Balancing

Application/Service

What do I get in visibility & telemetry?

Cloud Security Command Center



Finding & Assets



Pre request logging

Real time telemetry



Cloud Logging



Cloud Monitoring