Google Cloud

Modernize application delivery with Google Cloud's Global Front End

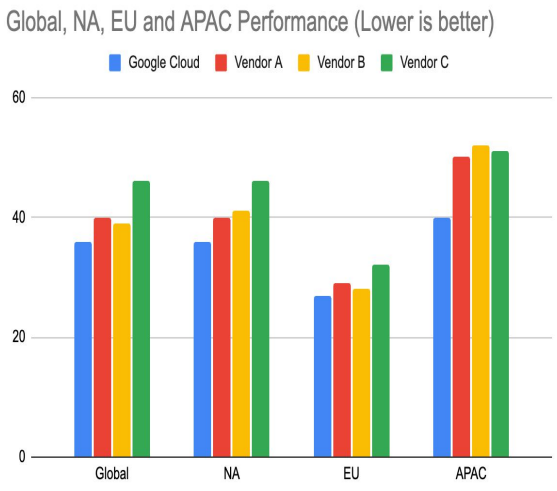
Modern internet-facing applications require global reach, performance, and high availability. Given most organizations are multicloud applications are often deployed across multiple cloud providers plus on-premises infrastructure. Managing a globally scaled web workload is incredibly challenging, especially when compounded by the complexity of microservice architectures where different origins address unique elements of the same overall web service. With this diversity of backend services comes an increased attack surface to protect. Customers are challenged to deliver high performance at scale while protecting their origins from web attacks and intrusions. Plus now with the rising use of AI, simplifying the front end to work seamlessly across any back-end will be critical.

Google Cloud offers a single front end solution capable of serving a broad set of web workloads. Our Global Front End offers a global network for low-latency web application delivery, auto-scaling capabilities for seamless resource management, simplified and secure connectivity to any backend, robust security measures for protection against DDoS and application attacks, exceptional reliability, and cost-effective pricing options with managed services for budget-conscious users. Services like Cloud Load Balancing, Cloud CDN, Cloud DNS, and Cloud Armor enhance the user and administrator experience by optimizing performance, availability, security, and global reach while Service Extensions enable broad extensibility and programmability.

Solution Benefits: Streamlining web application delivery with our unified Global Front End offers multiple benefit including :

- **Global Performance**

Boost your application's performance and global reach with our front end proxy solution. Leverage Google Cloud's massive network (202 points of presence) and premium infrastructure for low-latency connections and enhanced security. Cloud CDN further optimizes web and application performance by caching content closer to your users. See the results yourself: the chart below demonstrates object latency with real-user metrics (RUM) over 14 days.



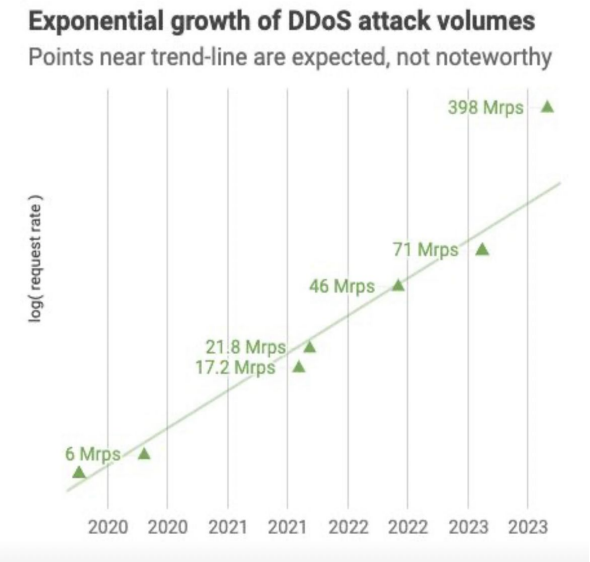
- **Planet Scale Security**

Cloud Armor provides always-on defense against common Layer 3 and Layer 4 network attacks. This protection is built-in and preconfigured for all Google Cloud projects using proxy load balancers. For sophisticated Layer 7 DDoS attacks, leverage adaptive protection powered by machine learning trained on your specific applications for tailored mitigation.

Cloud Armor safeguards your applications from DDoS and other web attacks, ensuring Layer 7 security whether you're running on Google Cloud, in a hybrid, or multicloud setup. It defends against attacks including, but not limited to:

- Direct botnet attacks
- UDP, SYN, TCP, DNS, and ICMP floods
- UDP amplification/reflection assaults

This power was demonstrated again in late 2023 when Cloud Armor successfully blocked the largest known DDoS attack, clocking in at 398M requests per second.



- **Scalable Open Traffic Control**

Make the application achieve high level of redundancy and availability while residing on any cloud or on-prem. The Google Cloud external Application Load Balancer allows you to group your backend resource, balance the workload across the group members, and provide the elasticity / scale for the components of the application.

The backend may be distributed across multiple region providing high resiliency and optimal load distribution. The newly introduced Service Extensions integration with our Global Front End enables you to make callouts to user-managed services during Cloud Load Balancing data processing. You write callout extensions against Envoy's external processing gRPC API. The backends for Service Extensions callouts run as general-purpose gRPC servers on user-managed compute VMs and Google Kubernetes Engine (GKE) pods on Google Cloud, multicloud, or on-premises environments.

- **Modern Automation**

The Dev(Sec)Ops toolkit provides an out-of-the-box, curated solution to accelerate the delivery of internet-facing applications. It combines Cloud Load Balancing, Cloud Armor, and Cloud CDN into one solution with support for Cloud Build or third-party CI/CD tools like Jenkins and Gitlab. The goal is to provide platform and DevOps engineers the ability to accelerate their Web deployments in the cloud.

How it works

A user requests a web page from the external Application Load Balancer, and if Cloud CDN is enabled and the content exists in the CDN cache (cache hit scenario), the request will be evaluated by Cloud Armor edge security policies. If Cloud CDN does not have the content in cache (cache miss scenario), the request will be evaluated by Cloud Armor backend security policies before being distributed to one of the backend servers. Once the content has been retrieved, it will be cached in Cloud CDN and this cached response will be served for future requests. Lastly, the external Application Load Balancer returns the web page content to the user.

Get started with Google Cloud's Global Front End

Modernize your application deliver and migrate your front end to our Global Front End.

Resources:

https://cloud.google.com/security/products/armor
https://cloud.google.com/cdn
https://cloud.google.com/dns/
https://cloud.google.com/load-balancing/docs/https
https://cloud.google.com/blog/products/networking/introducing-the-devsecops-toolkit