Grand Valley State University
www.gvsu.edu

Cloud Computing Geographic Issues

CIS437
Erik Fredericks // frederer@gvsu.edu

Adapted from Google Cloud Computing Foundations, Overview of Cloud Computing (Wufka & Canonico)

FIRST, SOME IN-CLASS WORK

In teams of ~3, come up with:

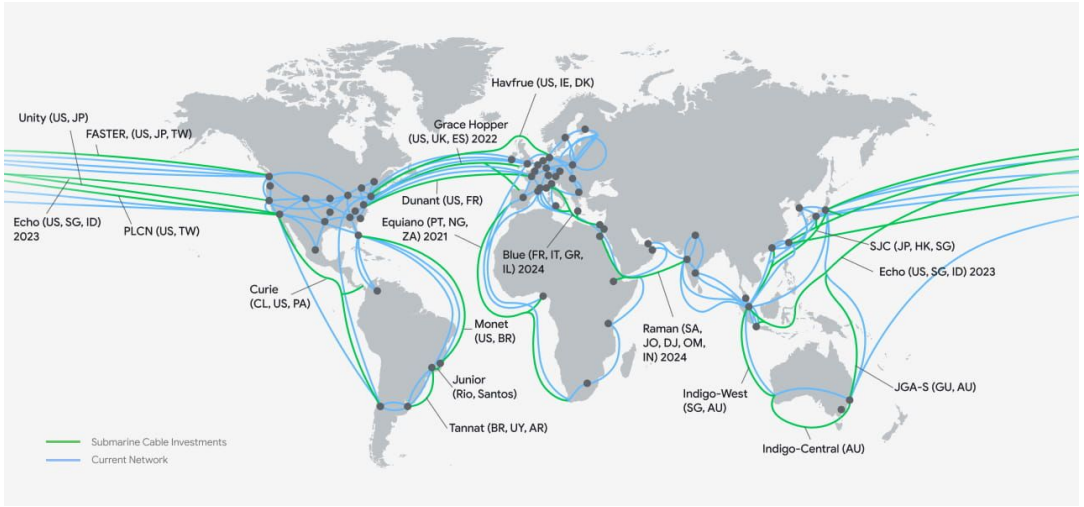
Three concerns that may arise from deploying apps globally

Location-based serving

Considerations:

- Where is data stored?
- Who can access it?
- Are we only optimizing for speed or is there … more to it?

Are these concerns? Why?



Consider:

Have been somewhat hand-waving location, but you've been *doing it all along!*

- *gasp*

Every time you create a service/VM/thing, you specify *where it is hosted*

Can you load balance or use "closer" regions to your clients?

- Sure, but you have to configure that (typically)!!

Data Residency / Transfer Policies

Data residency - where the data is stored

- Where would this be an issue?

https://www.microsoft.com/en-us/trust-center/privacy/data-location

Data Residency / Transfer Policies

Data residency - where the data is stored
- Where would this be an issue?

Private information
- Data we might be concerned about:
  - Medical
  - Financial
  - Military
  - ...
  - just plain old private data

Location-based serving

Location of Customer Data

"Microsoft provides strong customer commitments regarding cloud services data residency and transfer policies. Most Azure services are deployed regionally and enable the customer to specify the region into which the service will be deployed, e.g., the United States. This commitment helps ensure that Customer Data stored in a U.S. region will remain in the United States and will not be moved to another region outside the United States."

https://devblogs.microsoft.com/azuregov/managing-export-controls-in-azure-and-azure-government/

"Large-scale, multinational CSPs, often called hyperscale CSPs, represent a transformational disruption in technology because of how they support their customers with high degrees of efficiency, agility, and innovation as part of world-class security offerings. The whitepaper explains how hyperscale CSPs, such as AWS, that might be located out of country provide their customers the ability to achieve high levels of data protection through safeguards on their own platform and with turnkey tooling for their customers. They do this while at the same time preserving nation-state regulatory sovereignty."

https://aws.amazon.com/blogs/security/addressing-data-residency-with-aws/

Leaving off things like military/financial data

What about:

- GDPR (i.e., how websites/apps manage your data // your data privacy)?
- Serving ads to children?
- Gambling / lootboxes?

Different countries will have different rules!

- Do you:
  - Restrict access?
  - Serve different content to different regions?

Data Residency / Transfer Policies

Consider:

User A stores data in a cloud storage bucket (or virtual machine, or wherever they feel like storing data)

- User A does a terrible job with security

User B, perhaps some form of malicious actor, realizes that User A has set up a leaky storage solution and accesses their data

... not unheard of!

Da

Con

Use herever they
feel
-

Use s set up a
leak

... nc

SIGN IN / UP

The Register

SECURITY

This article is more than **1 year old**

Leaky AWS S3 buckets are so common, they're being found by the thousands now – with lots of buried secrets

When will this madness end?

47

Shaun Nichols in San Francisco

Mon 3 Aug 2020 / 23:47 UTC

Misconfigured AWS S3 storage buckets exposing massive amounts of data to the internet are like an unexploded bomb just waiting to go off, say experts.

The team at Truffle Security said its automated search tools were able to stumble across some 4,000 open Amazon-hosted S3 buckets that included data companies would not want public – things like login credentials, security keys, and API keys.

In fact, the leak hunters say that exposed data was so common, they were able to count an average of around 2.5 passwords and access tokens per file analyzed per repository. In some cases, more than 10 secrets were found in a single file; some files had none at all.

These credentials included SQL Server passwords, Coinbase API keys, MongoDB credentials, and logins for other AWS buckets that actually were configured to ask for a password.

That the Truffle Security team was able to turn up roughly 4,000 insecure buckets with private information shows just how common it is for companies to leave their cloud storage instances unguarded.

Though AWS has done what it can to get customers to lock down their cloud instances, finding exposed storage buckets and databases is pretty trivial for trained security professionals to pull off.

https://www.theregister.com/2020/08/03/leaky_s3_buckets/

All | Shorts | Videos | Unwatched | Watched | Recently uploaded | Live | Under 4 min | 4 - 20 min | Over 20 min | Filters

Web Hacking: How to Hack Amazon S3 Buckets

33K views • 8 years ago

Web Development Tutorials

In this web **hacking** video tutorial, I show you how I **hacked** HackerOne's AWS **S3 buckets** for a $2500 bounty. In it, I show you how ...

intro to cloud hacking (leaky buckets)

125K views • 1 year ago

NetworkChuck

In this video, you'll learn how to **hack** the cloud, specifically **Amazon S3**. We'll cover what **S3 buckets** are, security basics, how to ...

4:14 Let's start hacking. Now, before we can **hack Amazon S3** buckets, we gotta create one, know how it works, know how it ticks, let's ...

4K CC

Dumping S3 Buckets | Exploiting S3 Bucket Misconfigurations

36K views • 3 years ago

HackerSploit

In this video, we will take a look at how to perform reconnaissance on AWS **S3 buckets** and how to exploit **S3 bucket** permission ...

Leaky bucket?

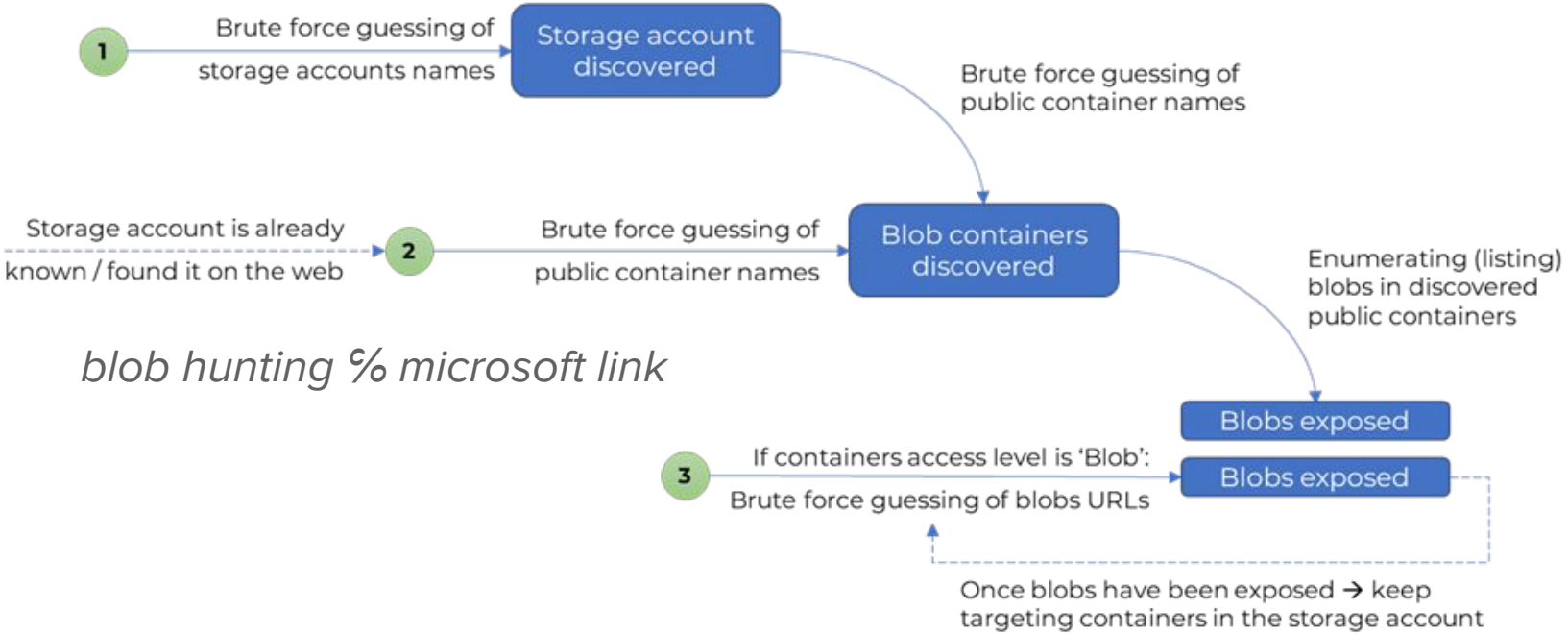
https://youtube.com/shorts/mdIjFA6oEYo?si=_jC0mWoTL_W9-SZD

How can we prevent "leaky buckets" or similar issues?

Suggestions

https://www.tenable.com/blog/leaky-amazon-s3-buckets-challenges-solutions-and-best-practices

https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/protect-your-storage-resources-against-blob-hunting/ba-p/3735238



blob hunting % microsoft link

Suggestions

Enable activity logging:

- AWS CloudTrail / (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html) / Cloud Audit Logs (GCP) / Activity Logs (Azure)

Continuously pentest

- Is your bucket accessible by somebody who shouldn't have access? Even internally?

Setup alerts for unexpected activities

Set a *lifecycle* for buckets

- Transfer data from old bucket to new bucket every so often
    - Why?

An example

https://www.youtube.com/watch?v=UB2KSBR3Zbk

Regions and Zones

Region:

- Geographical location for hosting resources
- Many worldwide
- e.g., us-east1

Zone:

- Part of region
- Typically, 3 or more zones per region
- e.g., us-east1-a

Holds for AWS and Azure too!

https://cloud.google.com/compute/docs/regions-zones/


1035 DI MASSEY FE
PLANETARY PLUS
40
KA 40
B-0516
Yasha Gowda
SRI LAKSHMI

Export Controls

https://www.bis.doc.gov/documents/bis-annual-conference-2018/2239-cloudy-with-a-chance-of-technology-transfer-breakout-rev-13may2018/file

(2024 updates include Russia, Belarus...)

Unfortunately a topic that continually comes up in many domains

- E.g., you can't bring a laptop to particular countries, if your data is available it must be scrubbed, etc.

So how do we handle this?

What are some options for limiting data access?

So how do we handle this?

What are some options for limiting data access?

- https://cloud.google.com/security/compliance/ear
- https://devblogs.microsoft.com/azuregov/managing-export-controls-in-azure-and-azure-government/

From Google:
"Customers with Export Administration Regulations (EAR)-regulated workloads are responsible for determining what steps (if any) are necessary to ensure that their use of the cloud is consistent with the EAR. If customers choose to deploy any of the above technologies to meet their EAR compliance requirements, customers have final responsibility to properly deploy and maintain them."

So how do we handle this?

What are some options for limiting data access?

So, it is up to you!

- Limit IP address ranges
- Enable access control (IAM)
- Restrict unapproved services (disable access when not needed)
- Store data locally (to your clients)

Sounds a lot like sysadmin rules - limit access to those who don't need it

- Good practice regardless ^

So how do we handle this?

What are some options for limiting data access?

- Additionally, **always monitor** who is accessing your data!
  - What do the logs say?

Other concerns

Leaving aside the export control, what about data privacy?

- Say, healthcare or financial records
- Many, many companies offload their data storage to the cloud

Something we'll talk more in the security module, but the quick answer:

1) Secure your services/buckets
2) **SECURE YOUR SERVICES/BUCKETS**
3) ...
4) Did you secure your services/buckets?
    a) Who has access to those buckets? And perhaps the services?
    b) Are you routinely monitoring access? Have triggers for when unexpected accesses occur?
    c) Are you logging?

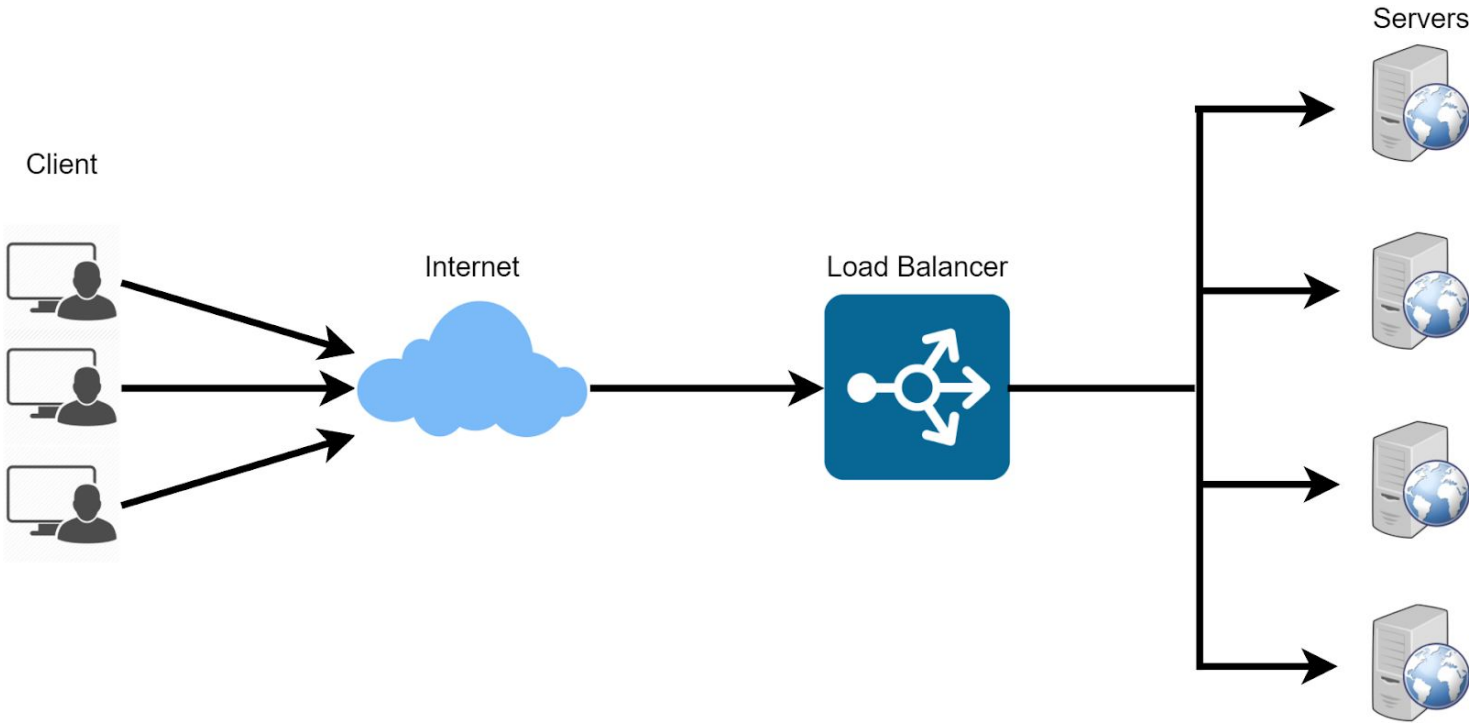
DIFFERENT DEMO!

Limiting by IP address/region?

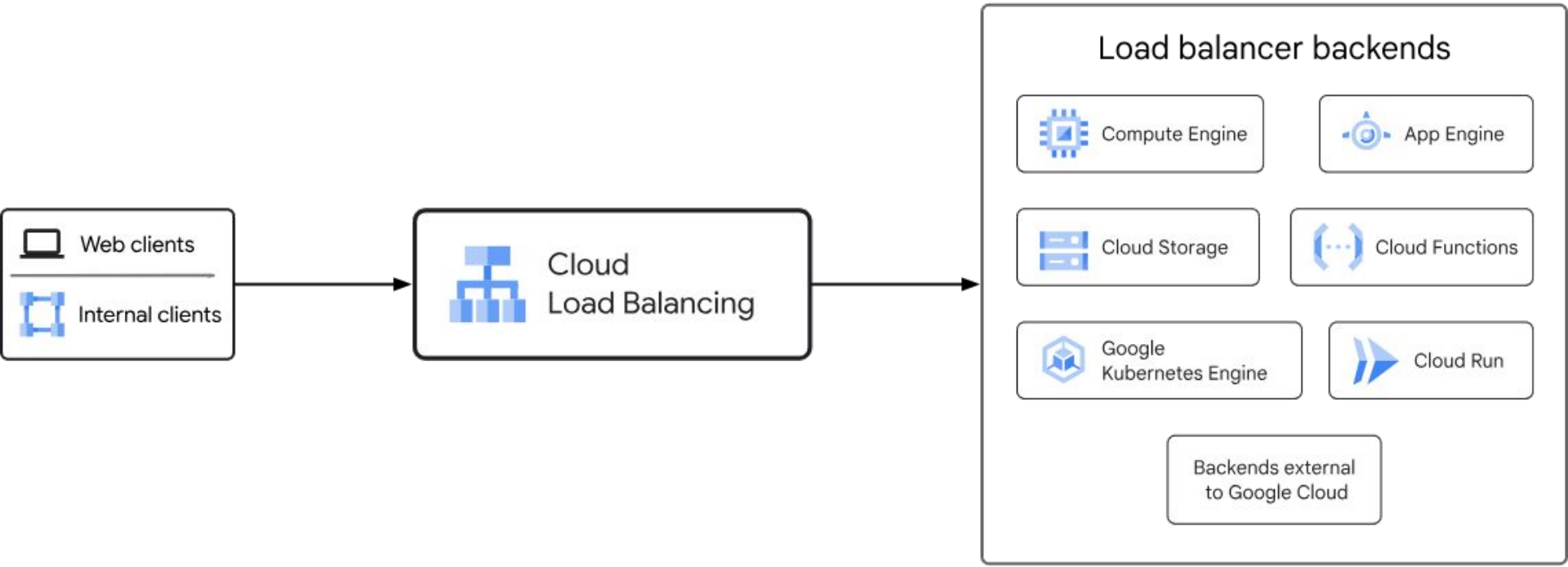
https://cloud.google.com/armor/docs/rules-language-reference#allow_or_deny_traffic_from_a_specific_region

Region-based load balancer
https://www.cloudskillsboost.google/focuses/642?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=38338573

Load Balancing



Load Balancing Demo



Load Balancer

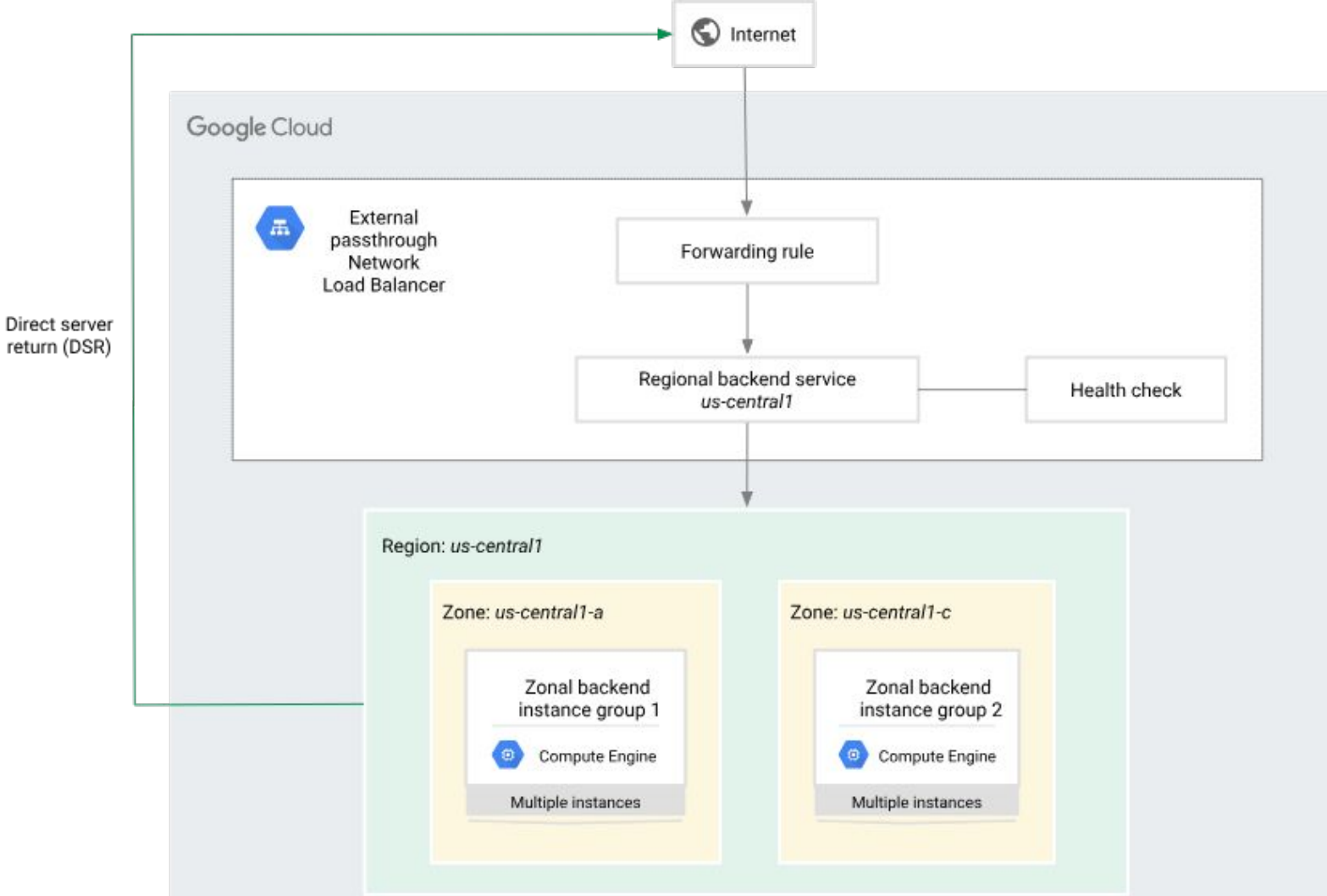
Note - this used to be something you'd have to manage yourself with heartbeat monitors, manually-configured failovers, etc.

- Now it is a cloud service

https://cloud.google.com/load-balancing/docs/network/setting-up-network-backend-service

Similar to the load balancer we did before

- Balances traffic across two separate regions


Internet
Google Cloud
External passthrough Network Load Balancer
Forwarding rule
Regional backend service
us-central1
Health check
Direct server return (DSR)
Region: us-central1
Zone: us-central1-a
Zonal backend instance group 1
Compute Engine
Multiple instances
Zone: us-central1-c
Zonal backend instance group 2
Compute Engine
Multiple instances