Design for security

Architecting with Google Cloud Platform: Design and Process

Last modified 2018-08-08

© 2017 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

"We thwart adversaries by ... anticipating them, preventing them, detecting them, disrupting them, and containing them... and ensuring that you can leverage our security capabilities on top of the platform. Trust is created through transparency, not just technology."

--- Neils Provos,
Google Distinguished Engineer

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

https://pixabay.com/en/chainlink-fence-metal-wire-690503/

Agenda

Cloud security

Network access control and firewalls

Protections against denial of service

Resource sharing and isolation

Data encryption and key management

Identity access and auditing

Photo service: Intentional attack.

Design challenge #5: Defense in depth

No GCP lab in this module

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Cloud security

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Google's strategy for cloud security is pervasive defense in depth

Transparency

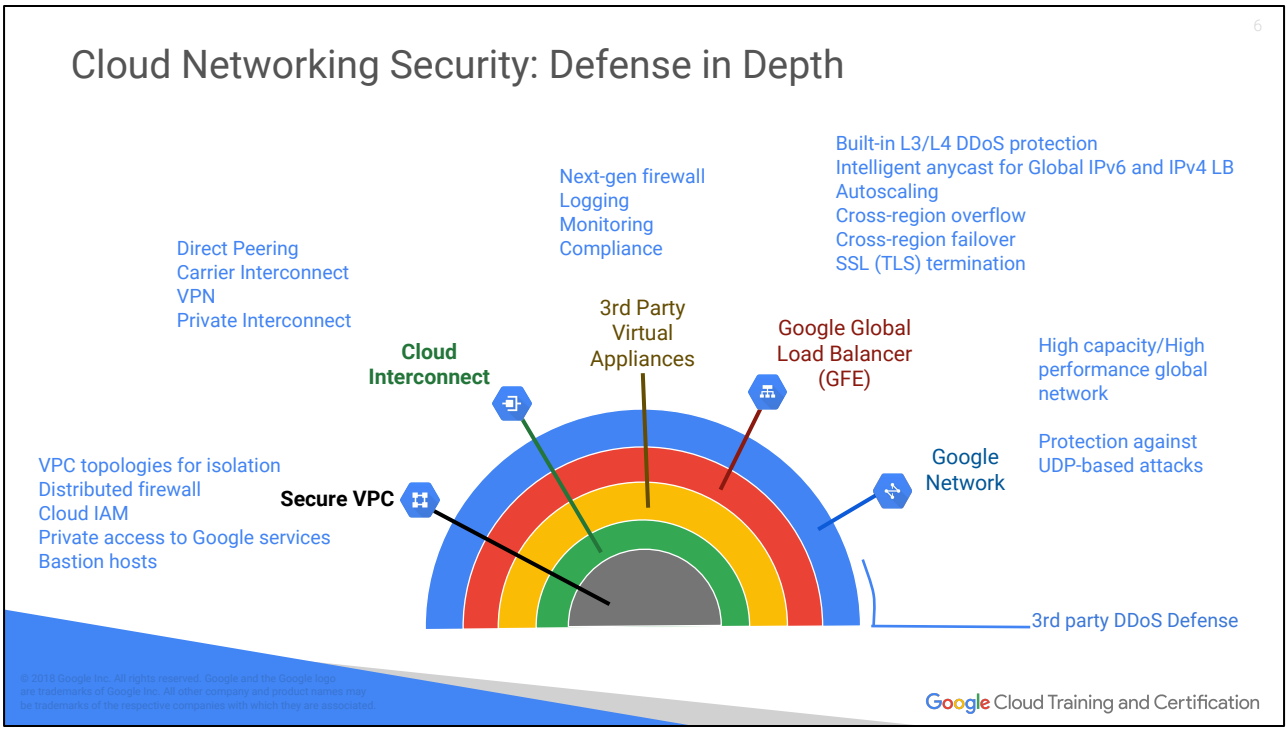
- Explain which parts Google is doing and which are yours
- Give you the tools and access to monitor your service
- Give you the controls and features needed to leverage platform security

Segregation of duties

- What is provided by the platform?
- What are you responsible for?

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Principle of least privilege: The user is granted only the privileges that are essential to that user's tasks.
https://en.wikipedia.org/wiki/Principle_of_least_privilege
Segregate these duties: Key management, Application change control, Security configuration change management. And where you can't segregate, compensate and document.
Defense in depth: Overlapping layers of security. Provide redundancy in case a security control fails.
https://en.wikipedia.org/wiki/Defense_in_depth_(computing)
Transparency: Provide cloud security services with visibility and controls. 1) Explain what Google is doing. 2) Give you the tools/access to monitor it for your application. 3) Give you the controls and features needed to customize elements as required.
https://cloud.google.com/security/
Google transparency report: https://transparencyreport.google.com/



Layers of protection. Each layer protects and complements the next internal layer.

- **Secure VPC:** Identify optimal VPC topology. Deploy distributed firewalls. Control access with IAM permissions. Avoid adding Public IPs to instances. Access Google services internally.
- **Cloud Interconnect:** Connect securely to on-prem or other-cloud deployments. Private Interconnect. Carrier Interconnect. Direct Peering. VPN.
- **3rd Party Virtual Appliances:** Enhance VPC security with 3rd party appliances. Next-gen firewalls. IDS/IPS (intrusion detection). Logging. Monitoring. Scale 3rd party appliances using internal load balancing so you don't create choke points in your VPC.
- **Global Load Balancing** provides edge protection and global infrastructure protection for IPv4 and IPv6. Layer 3 and 4 DDoS protection. Anycast IP - even if backends are in multiple regions. To absorb attacks for resiliency - autoscaling, cross-region overflow, and cross-region failover.
- **Google Network:** High capacity. High performance. SDN network virtualization Global networks with subnets. Organization, folders, cross-project networking, peering.
- **3rd Party DDOS:** You can complement this infrastructure with additional DDoS security from 3rd party providers.

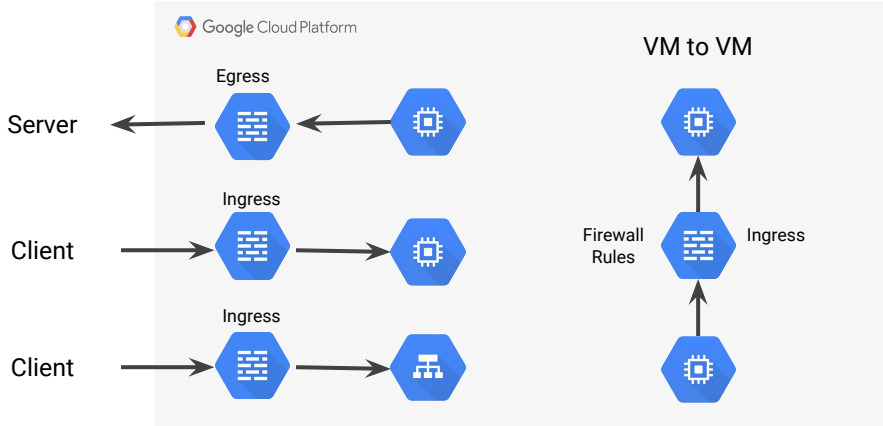
Network access control and firewalls

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Google Cloud Training and Certification

https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#a_virtual_firewall_and_routes_control_all_network_access

Firewall configuration is the first line of defense for access



- Ingress and Egress firewall
- Permit/Deny
- Stateful with Connection tracking
- Distributed: enforced on host => no choke points

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Encrypt all access to VMs over public IPs.
Restrict all traffic to a network or to a set of target machines to specific ports, source IP ranges, or specific source IP addresses.
Separate Control: Internet-to-Frontend and VM-to-VM with routes and firewall rules.
Use Tags: Build rules using Tags so that they are applied to VMs as they boot.

Choke point: In a physical network a choke point is a location in the network where congestion can accumulate and overrun a device. For example, a hardware firewall can only drop traffic at the line rate of the firewall device. Hammering that device with bad traffic to be dropped could reduce or inhibit good traffic getting through, causing a performance issue or a denial of service. In GCP, the virtual firewall function is distributed. Traffic is dropped at the host. GCP firewalls are designed to eliminate choke points.

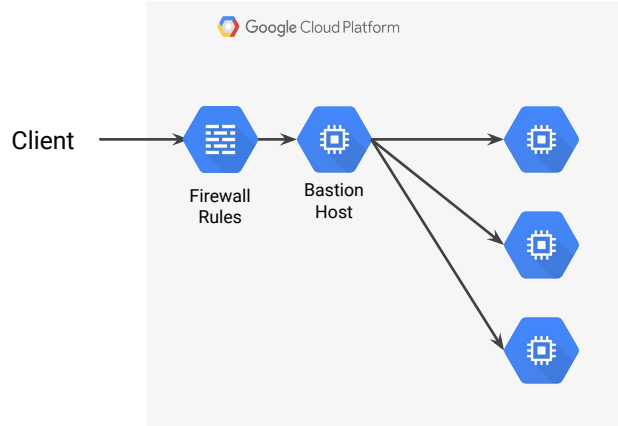
Designs for securely accessing VMs

VMs with external IP addresses

- Compute Engine firewalls
- HTTPS and SSL
- Port forwarding over SSH
- SOCKS proxy over SSH

VMs without external IP addresses

- Bastion hosts and SSH forwarding
- IPSec VPN
- NAT gateway for egress
- Interactive serial console access



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

https://cloud.google.com/solutions/connecting-securely

Topology: Project, Network, Subnetwork (IP Range)
Internal interface
Public interface
Multiple NIC
Alias IP Ranges
Routes
Host-based filtering (iptables)
Tunneling (VPN)

API access control using Cloud Endpoints

Develop, deploy, protect and monitor your APIs that are used by mobile and web clients.

Control who has access to your API and validate every call with JSON Web Tokens and Google API keys. Integration with Auth0 and Firebase Authentication lets you identify the users of your web or mobile application.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Protections against denial of service

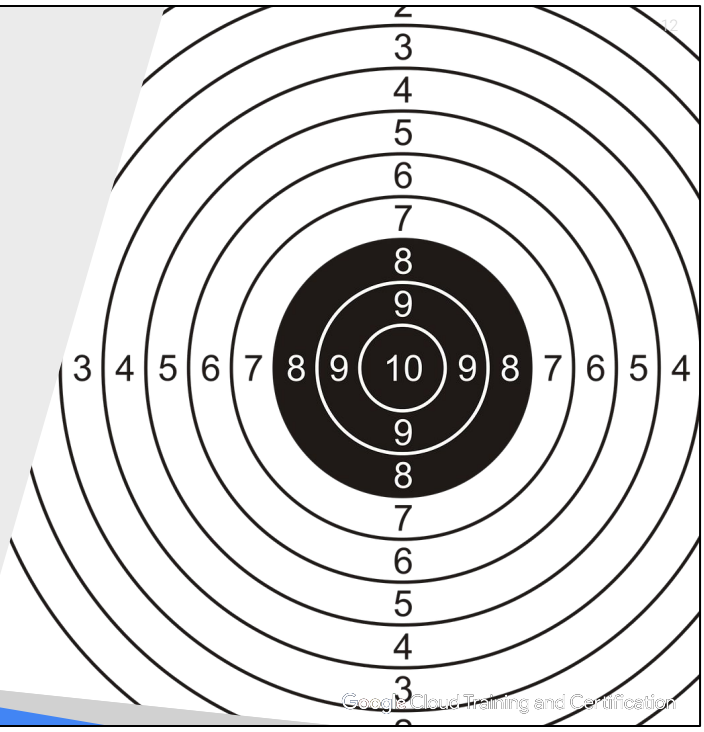
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

DDoS

Distributed Denial of Service Attack

An attempt to exhaust resources to deny service to you users.

- Bandwidth
  - Consume bandwidth with volume of traffic
- Connection
  - Exhaust connection state tables
- Application
  - Exploit application limitations

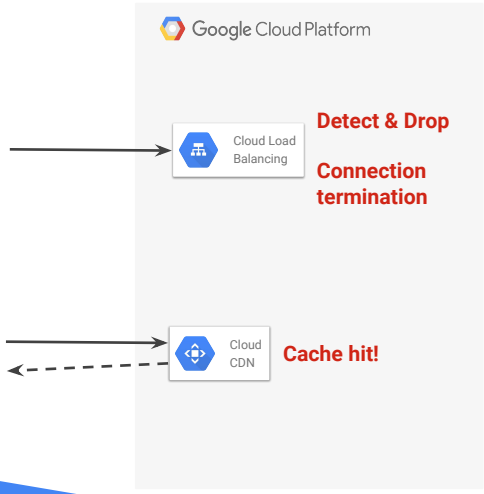


© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

OSI Model Layers
Bandwidth: also called a Network or Layer 3 attack
Connection: also called a Layer 4 attack
Application: also called a Layer 7 attack

https://pixabay.com/en/shield-infantry-shield-shooting-2360743/

Edge protections against DDoS



TCP/SSL Proxy

- Drops all UDP floods
- Solves SYN floods by terminating the TCP connection.

Global Load Balancing

- Detects and drops source port UDP
- Solves NTP amplification
- Bandwidth protection and Connection protection

Cloud CDN

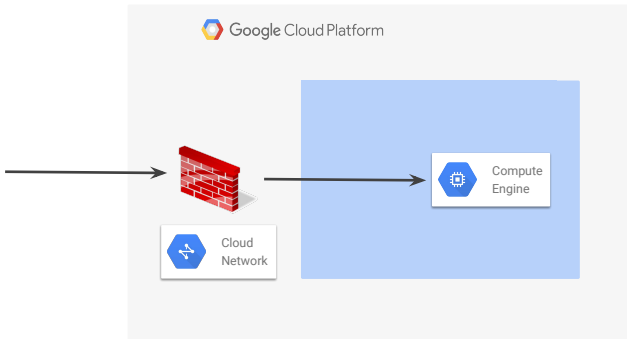
- Content is served from the edge
- Cache hit insulates the network and your application

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Connection protection: HTTP/HTTPS load balancing protects against connection-based attacks such as slowloris
Dropped traffic does not count against VM traffic limits

Google also partners with 3rd party providers to offer additional DDoS protection.

Network protections against DDoS



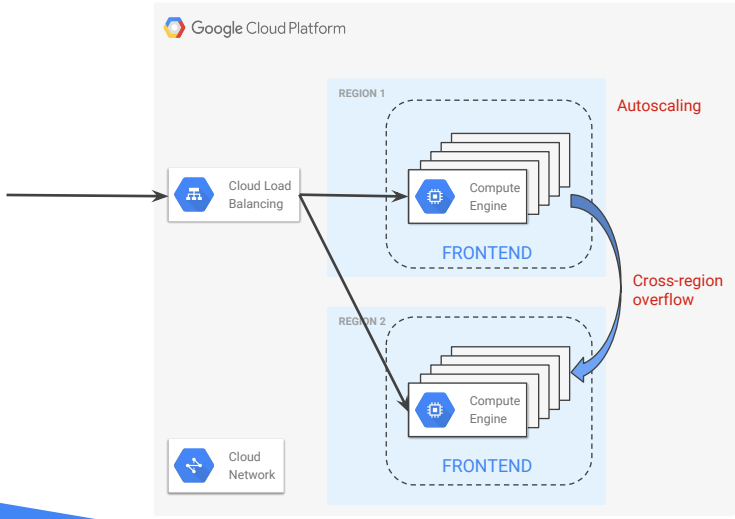
Cloud Network Firewall

- Filter known bad traffic before it reaches your application
- Cloud Armor offers IP blacklist/whitelist for HTTP(S) Load Balancing [beta]

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Cloud Armor's support for IP blacklisting and whitelisting for HTTP(S) Load Balancing is in beta at the time of this writing. That means that it is not covered by an SLA and it may change in backwards-incompatible ways.

Infrastructure protections against DDoS



Autoscaling

- Absorb attacks of any size
- Traffic throttling protects VMs

Cross-Region Overflow

- Failover to absorb attack

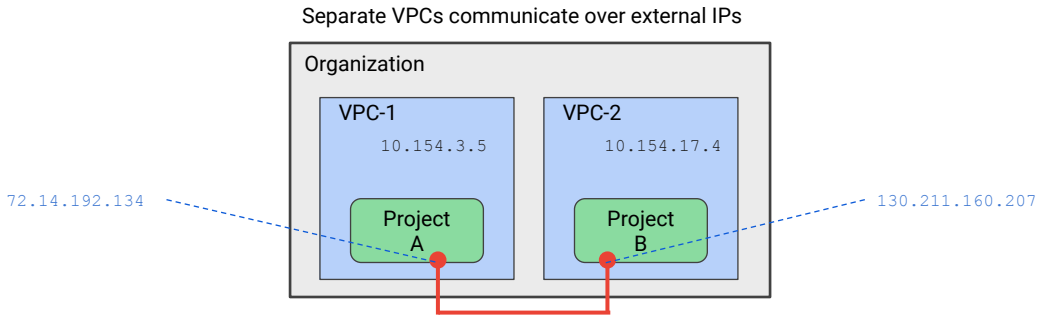
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Resource sharing and isolation

Sharing enables collaboration between parts, while isolation prevents the compromise of one part from spreading to other parts.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Virtual Private Cloud (VPC) isolation through public IPs

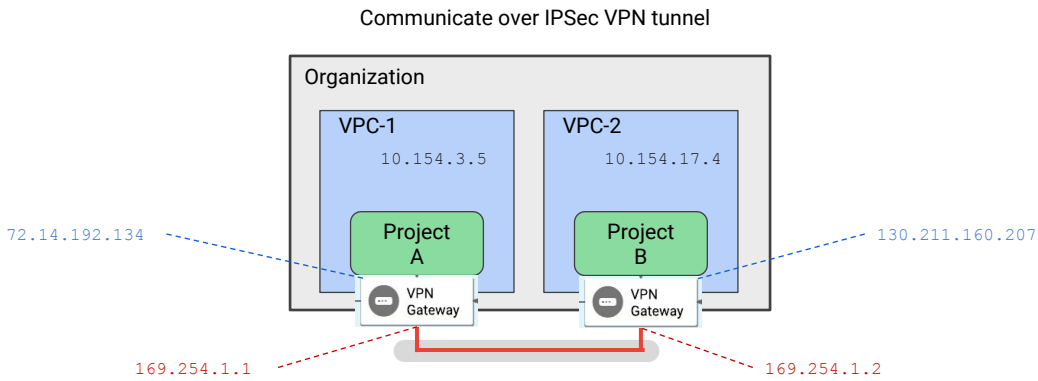


- VPC Network Isolation - Public IP
- Multiple projects grouped under org node but projects and virtual private networks are isolated
- Each projects has its own IAM control
- Communication occurs over Public IPs

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Public IP Addresses: https://cloud.google.com/compute/docs/configure-ip-addresses

IP address isolation and VPN tunneling



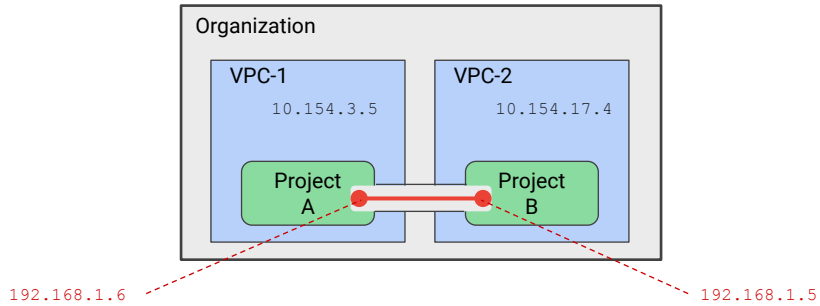
For increased privacy, the VPCs can communicate over VPN tunnels.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Virtual Private Network: https://cloud.google.com/compute/docs/vpn/creating-vpns

Cross-project VPC network peering

VPCs communicate over Private RFC1918 Address Space



Projects are isolated in separate VPCs, but using network peering they can communicate over a private address space.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Once networks have peered, every internal, private IP is accessible across peered networks. VPC Network Peering does not provide granular route controls to filter out which subnet CIDRs are reachable across peered networks. You must use firewall rules to filter traffic if such filtering is needed. The following types of endpoints/resources are reachable across directly peered networks:

- Virtual machine (VM) internal IPs in all subnets
- Internal load balanced IPs in all subnets

The following types of endpoints/resources are NOT propagated to directly peered networks:

- Static routes
- VPNs

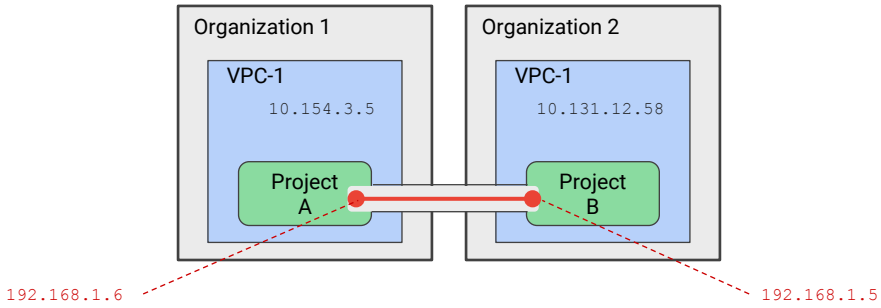
VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks, including:

Network Latency: Public IP networking suffers higher latency than private networking.
Network Security: Service owners do not need to have their services exposed to the public Internet and deal with its associated risks.
Network Cost: GCP charges egress bandwidth pricing for public IPs even if the traffic is within the same zone. Services running in a GCP network that do not need to be accessed over public IPs do not need to pay for those egress costs.

VPC Network Peering Limits: 25 direct peer networks, 7500 instances (peering and non-peering) per network, 50 forwarding rules

Cross-organization VPC network peering

VPCs communicate over Private RFC1918 Address Space

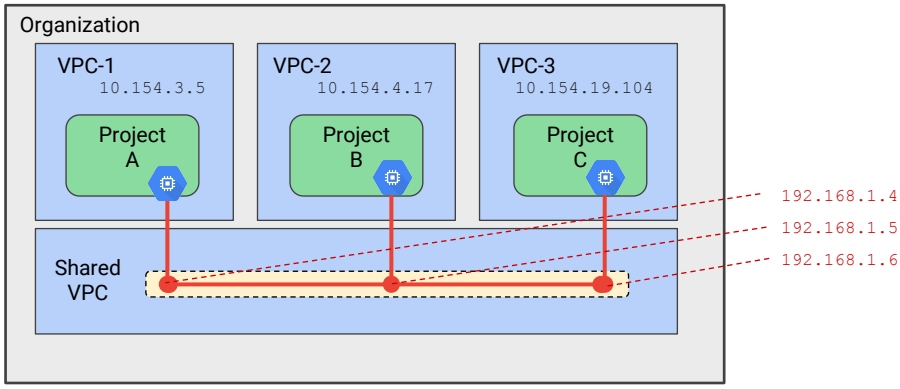


Works across organizations.
Organizations with several network administrative domains.
Organizations that want to peer with other organizations.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Shared VPC

Server in A provides service to clients in B and C



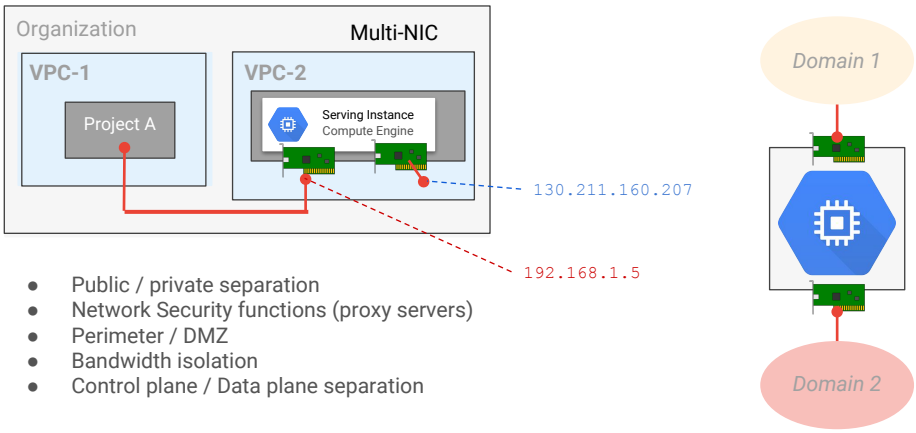
- Instead of a VPC being within a single project, Shared VPC allows the VPC to exist in multiple projects
- Useful for a service that must use resources from separate projects for independent accounting and billing

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

VPC Network Isolation - Public IP
Multiple projects grouped under org node but projects/networks are isolated.
Each projects has its own IAM control.
VPN tunnel between VPCs
XPN Cross Network Sharing
One XPN VPC with multiple projects
VPC Network Peering
Service account permits sharing of specific resources from one project to another
Multi NIC

https://cloud.google.com/compute/docs/vpc/vpc-peering

Isolation through multiple network interfaces



- Public / private separation
- Network Security functions (proxy servers)
- Perimeter / DMZ
- Bandwidth isolation
- Control plane / Data plane separation

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

You use separate interfaces to separate different domains and isolate their traffic.

You can have up to 8 interfaces on a VM, depending on the VM size/configuration.
Applications:
Perimeter
Multiple Network Interfaces:
https://cloud.google.com/compute/docs/multiple-interfaces-concepts

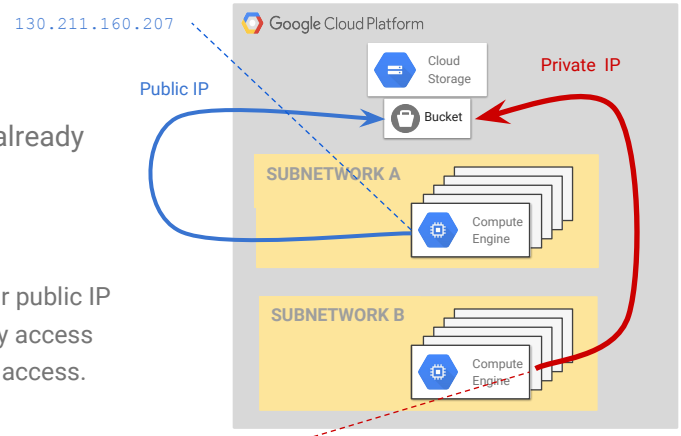
Access GCP services over internal IP

Google Private Access

Does not affect existing resources that already use External IPs

Example

- VMs on subnet A access the bucket over public IP
- VMs on subnet B have no public IP. They access the bucket over internal IP using private access.




```
gcloud compute networks subnets update
subnet-b \
    --enable-private-ip-google-access
```

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

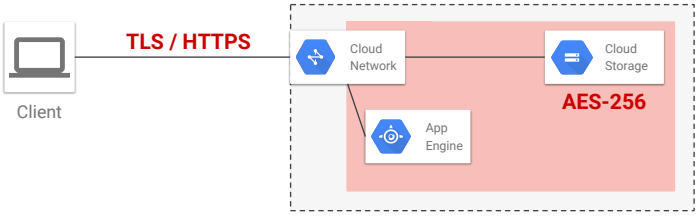
https://cloud.google.com/compute/docs/private-google-access/private-google-access
See latest list of supported APIs and services at the link. Currently Cloud SQL is NOT supported.
Cost of using a service is not changed by going over internal IP instead of external IP.

Data encryption and key management

Google encrypts all data in motion and all data at rest.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

GCP provides server-side encryption



- **Encrypted at rest by default**
- AES-256
- Keys are encrypted by Master keys
- Keys are automatically periodically rotated
- On-the-fly decryption by authorized user access with no visible performance impact
- Metadata is **not** encrypted *except:*
  - CRC32C Checksum
  - MD5 Hash

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Server-side encryption refers to data that has been received by Google Cloud Storage, and is encrypted prior to being stored.

https://cloud.google.com/storage/docs/encryption
https://cloud.google.com/storage/docs/using-encryption-keys
https://cloud.google.com/security/encryption-at-rest/

- Never store original passwords, only the hashed and salted values.
  - **Hash:** A special mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size and is a one-way function, that is, it cannot be inverted.
  - https://en.wikipedia.org/wiki/Cryptographic_hash_function
  - **Salt:** Random data that is used as an additional input to a one-way function that "hashes" a password or passphrase.
  - https://en.wikipedia.org/wiki/Salt_(cryptography)
- Automate key management; rotate keys every 1-3 years
- Develop processes / playbook for security; behavior is as important as the technology
- Document the key lifecycle
- Guard keys against unauthorized access, both physically and digitally.
- Strong access control of keys, auditing, logging, and monitoring of access attempts

- Segregate duties: No individual should be able to create, manage, and use keys
- If security is breached, act quickly to regenerate and replace keys.

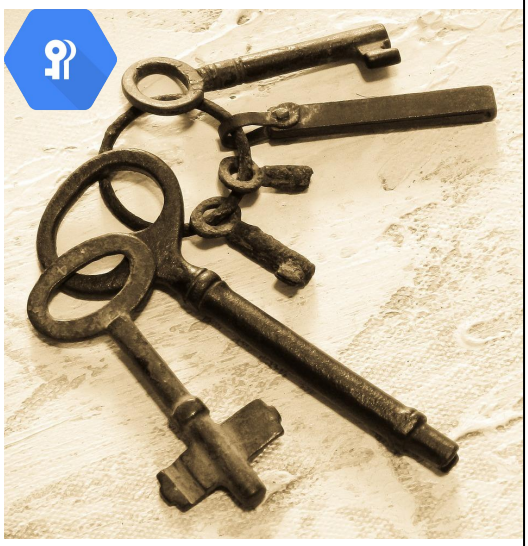
https://pixabay.com/en/key-close-security-open-castle-2510672/

Customer Supplied Encryption Keys (CSEK)

Use your own AES-256 in Standard Base 64 encryption keys with GCP services .

Keep keys on premise, and use them to encrypt your cloud services. You provide the keys as part of API service calls.

GCP uses the key in memory and does not write it to storage



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Not currently supported by Cloud Storage Transfer Service, Dataproc, Dataflow.
Not available in all locations.

https://pixabay.com/en/keys-keyring-vintage-antique-175759/

Persistent Disk Encryption with CSEK

Data is encrypted before it leaves your instance to travel to a persistent disk. You can provide your own CSEK keys.

Each disk remains encrypted with system-defined or customer-supplied keys

Persistent disk data is automatically distributed across physical media

When a persistent disk is deleted, the cipher keys are discarded, rendering the data irretrievable and the deletion process is irreversible.

If the key is lost, there is no way for Google to decrypt the disk or recover the data

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

https://cloud.google.com/compute/docs/disks/customer-supplied-encryption

The distribution of persistent disk data over physical media may add to the security of the data because it is not necessarily stored contiguously.
However, this part of the storage process is not user accessible. It is automatic and you can't change how the distribution works or bypass it.
https://cloud.google.com/compute/docs/disks/

https://pixabay.com/en/hard-disk-technology-electronics-42935/

Need more control over encryption?

Client-side encryption

You encrypt the data on premise or in your own application before it is sent to Google Cloud Storage and decrypt it after it has been retrieved

Disk encryption

If you want more or different controls than are provided by Persistent Disk Encryption, you can create your own persistent disks and (redundantly) encrypt them yourself

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Identity access and auditing

Identity and Access Management

Service Accounts

Standards Compliance

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

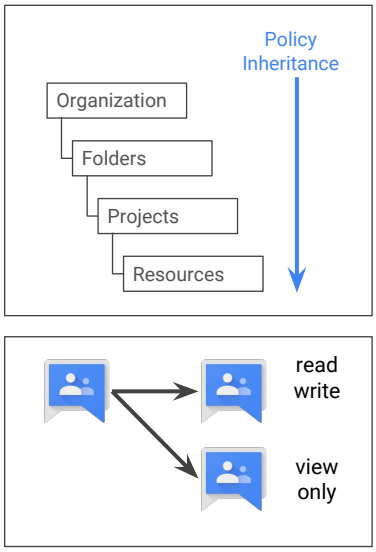
IAM policies

Grant roles to Google groups rather than individuals

- Groups can be more granular than job roles
- Use multiple groups for better control (such as *view only*)

Roles

- Prefer pre-defined roles over primitives / custom roles
- Grant roles at the smallest scope needed (least privilege)
- Limit use of “owner” role
- Consider hierarchy inheritance when assigning roles



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

https://cloud.google.com/iam/docs/overview

Standard Identity and authentication practices:

- Properly authenticate all services and people once a quarter. Use multifactor authentication.
- Unique usernames and no sharing of identity.
- Strong passwords.
- Prevent unauthorized entry. TLS, SSL, multifactor, 30m inactivity, 4h login

Update group membership instead of changing Cloud IAM policy. Audit membership of groups used in policies. Control the ownership of the Google group used in IAM policies.

- Use projects to isolate resources, and group resources that share the same trust boundaries
- Use networks within projects to isolate groups of VMs
- Move assets closer for lower latency, further away for disaster recovery
- Use network-local DNS for VMs to find one another (so they don't have to use an Internet service which might reveal internal topology/addresses)

Service accounts

VM can be authorized without holding the key, so its security is not compromised.

Best practices

- Grant the service account only the minimum required for purpose
- Create service accounts for a specific service
- Give the service account a meaningful display name
- Implement key rotation policy and auditing for service accounts

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

GCP security auditing with Forseti-security (open source tool)

Scans GCP projects in your organization for Cloud IAM policy.

Alerts if projects deviate from known-good policy.

Track environment with recurring resource snapshots, providing a history of cloud resources.

- Provides a history of cloud resources.
- Monitor access policies.
- Verify settings.
- Enforce safe settings and protect against unsafe changes.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

https://opensource.google.com/projects/forseti-security

Policy Scanner keeps the policies in your organization's Cloud Platform projects secure by:

Scanning Cloud Platform Projects in your organization
Alerting if scanned projects deviate from a known-good policy
Policy Scanner also allows you to create source-controlled repository of your projects' desired policies, and get alerts every time a project's policy doesn't match its intended value.

Cloud Audit Logging

All GCP services write audit logs

- Admin activity
- Data access

Who did what, where, and when?

Logs are kept for 7 days (or 30 days Premium)

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Google Cloud Platform services write audit log entries to these logs to help you answer the question of "who did what, where, and when?" within your Google Cloud Platform projects.

https://cloud.google.com/logging/docs/audit/#services

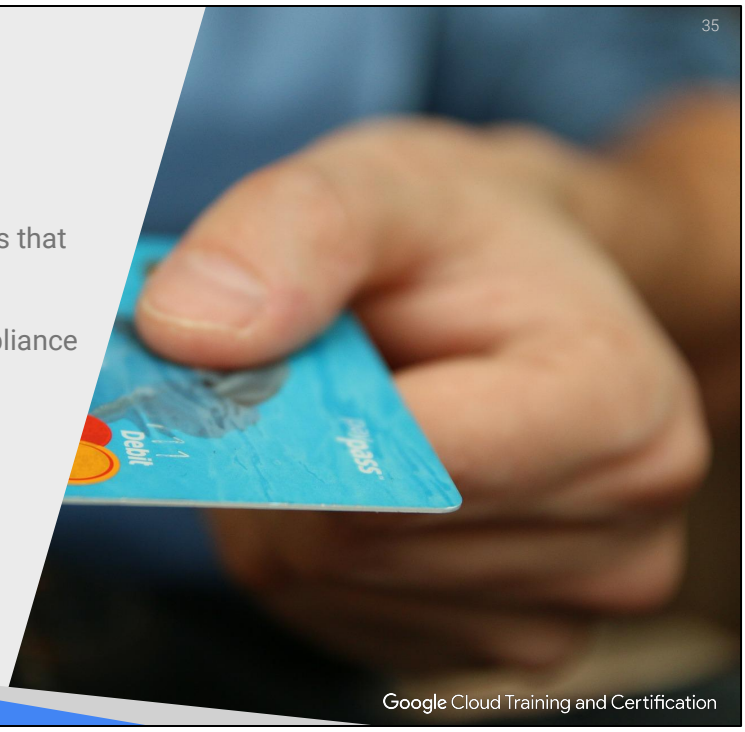
You can view audit log entries in your project's Activity Feed, in the Logs Viewer, in the Stackdriver Logging API, and in the Cloud SDK. You can also export audit log entries to Cloud Storage, BigQuery, or Cloud Pub/Sub.
https://cloud.google.com/logging/docs/audit/

https://pixabay.com/en/human-look-magnifier-man-2412988/

External audits and GCP standards compliance

You can find the detailed list of standards that GCP complies with here:

https://cloud.google.com/security/compliance

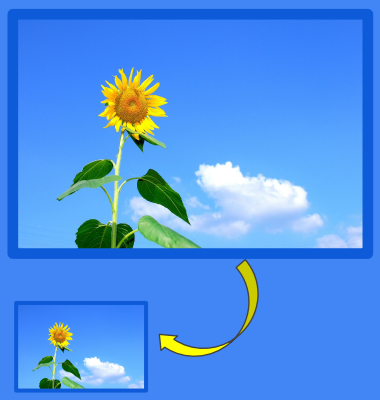


© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Google Cloud Platform maintains compliance with several standards.
For the latest information, look online:
https://cloud.google.com/security/compliance

https://pixabay.com/en/money-card-business-credit-card-256319/

Intentional attack



Is user privacy at risk?

Could a denial-of-service happen?

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

https://pixabay.com/en/summer-sunflower-flowers-sky-cloud-368224/

Hackers attack!

During a routine audit evidence was found in the logs that hackers are trying to gain access to the service.

What protections are already in place due to the choice of platform or the current design?

What steps can be taken to make sure user data is not already compromised?

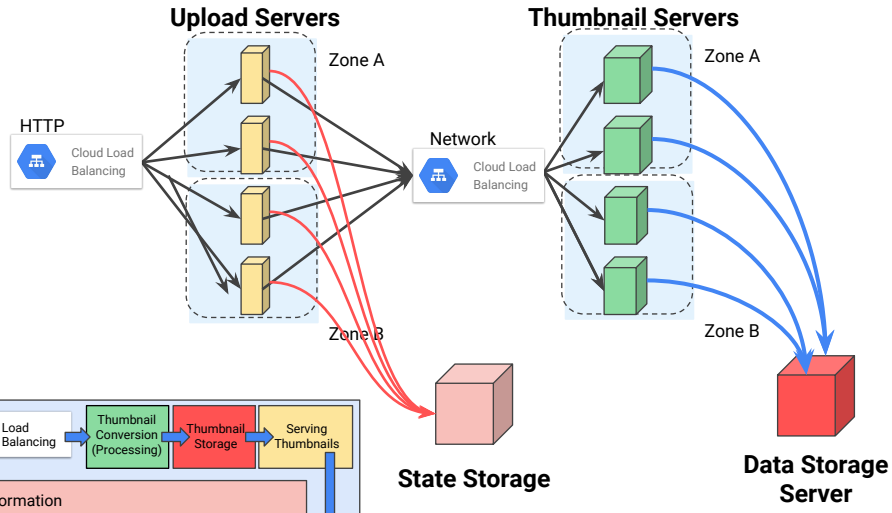
What additional design changes will reduce the "attack surface"?

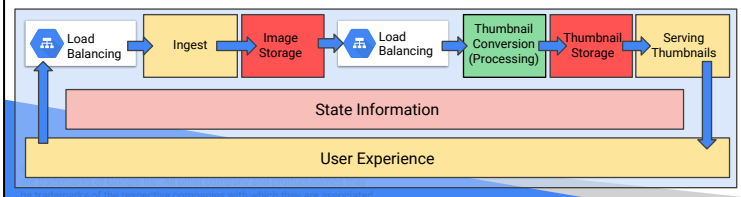
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Hackers attack!

Business Issue: Security vulnerabilities

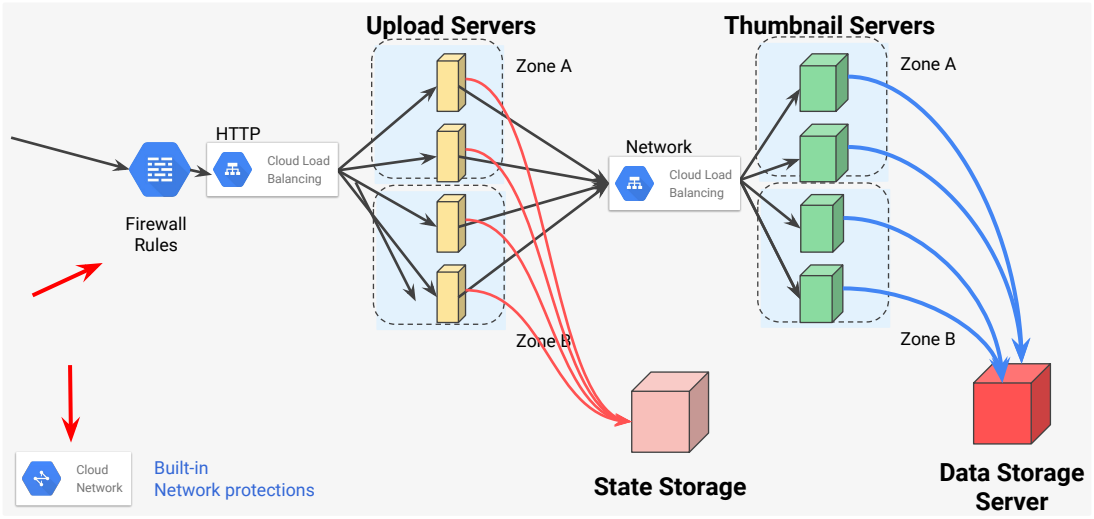
- Need to provide defense against hackers compromising privacy





be trademarks of the respective companies with which they are associated.

Lock down the front end



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Log data reveals they may be trying to hack.
CDN for cache protection.

1. Get all the protections of Cloud Network from Google.
2. Cloud load balancing detects and drops (DDos). Terminates connection (hacker)
3. Cloud CDN helps mitigate DDoS and reduces need to autoscale clusters.

Firewall to prevent hackers. (Found evidence in log)
Autoscaling.

Denial of service attack!

The service has been taken down by a Distributed Denial of Service (DDoS) attack!

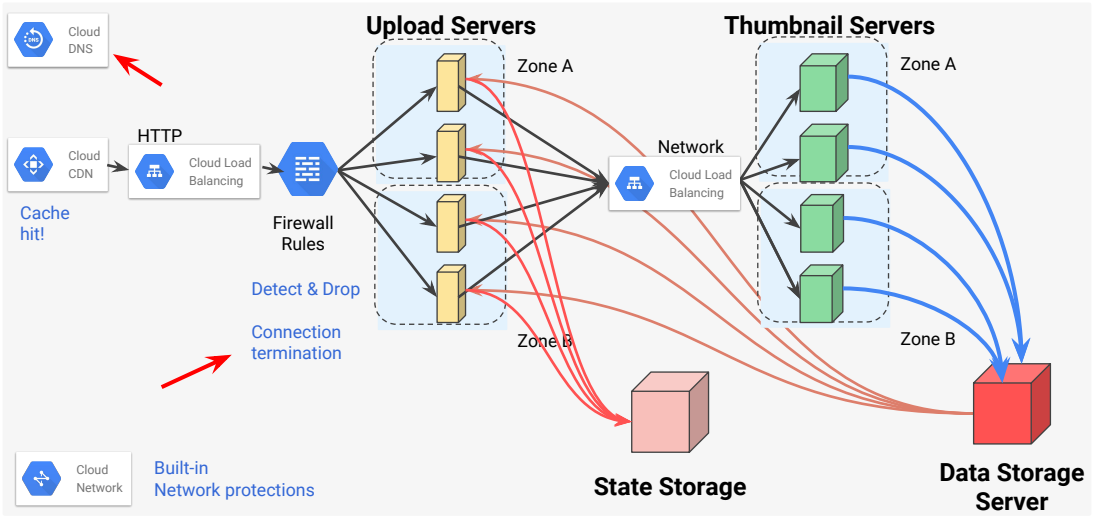
What processes are in place to deal with this?

Handle the immediate situation.

Then continue to evolve the design to protect against DDoS.

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Denial of Service attack! Cache, NW, LB



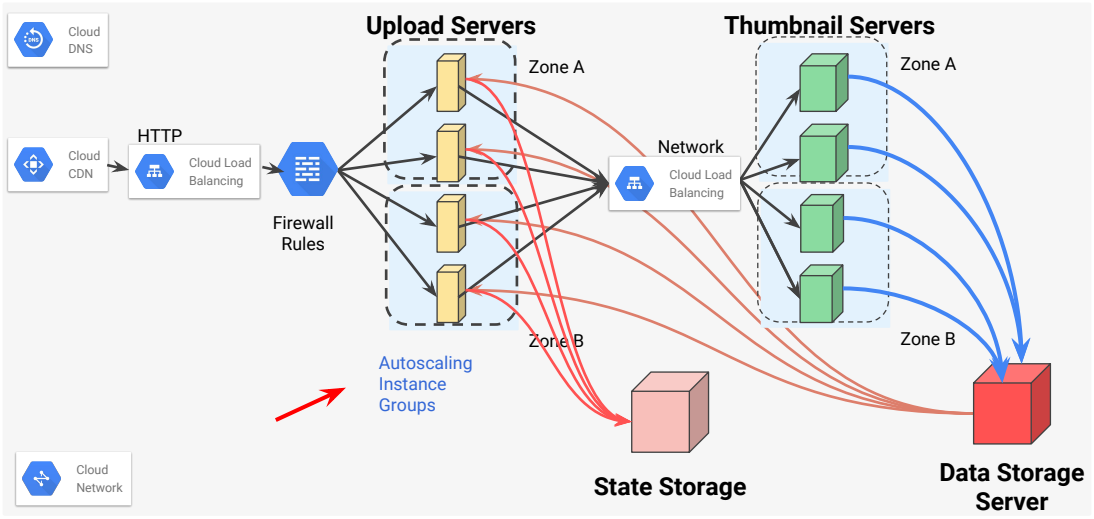
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Log data reveals they may be trying to hack.
CDN for cache protection.

1. Get all the protections of Cloud Network from Google.
2. Cloud load balancing detects and drops (DDos). Terminates connection (hacker)
3. Cloud CDN helps mitigate DDoS and reduces need to autoscale clusters.

Firewall to prevent hackers. (Found evidence in log)
Autoscaling.

Denial of Service attack! Autoscale



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

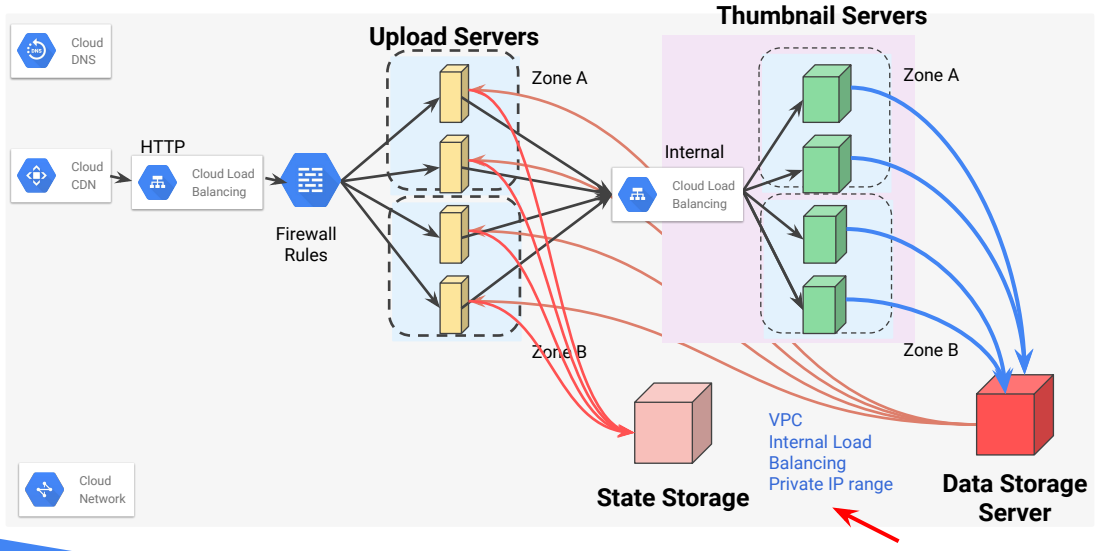
Hackers...

You locked down the front end to prevent hackers from gaining access to the service and potentially to sensitive user information. However, if they get around these protections, the back end servers are still vulnerable.

What design changes can you make to the back end to provide "defense in depth"?

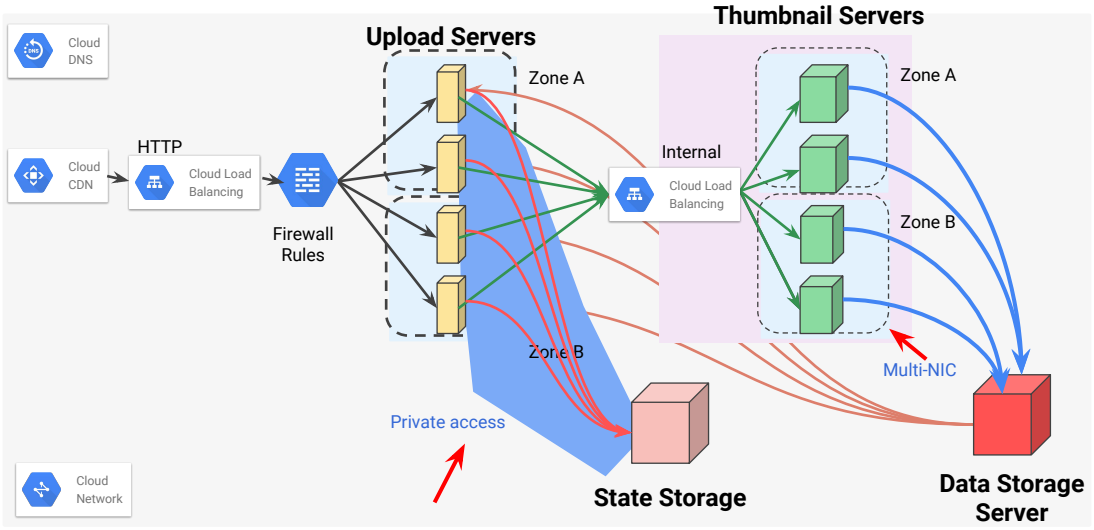
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Lock down the back end. VPC, Internal LB, Private IP



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Lock down the back end. Private access, Multi NIC



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Refer to slide 22 in this module for additional reasons to use multiple NICs in an instance.
Also, refer to the online docs for Multiple Network Interfaces:
https://cloud.google.com/compute/docs/multiple-interfaces-concepts

Security checklist:

- The original design had no firewalls
- The scalable and reliable elements were not in separate zones
- There was assumed implicit trust between all components
  - Added load balancers for protection
  - Consider using security accounts / bastion hosts to limit access
- Consider additional data encryption options such as creating and supplying keys
- Define operations / administration interface and functions
  - Define processes, playbooks, documentation, and training
  - Define groups and IAM roles
- Define testing elements and processes for testing and verifying security

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

YOUR TURN

Design challenge #5

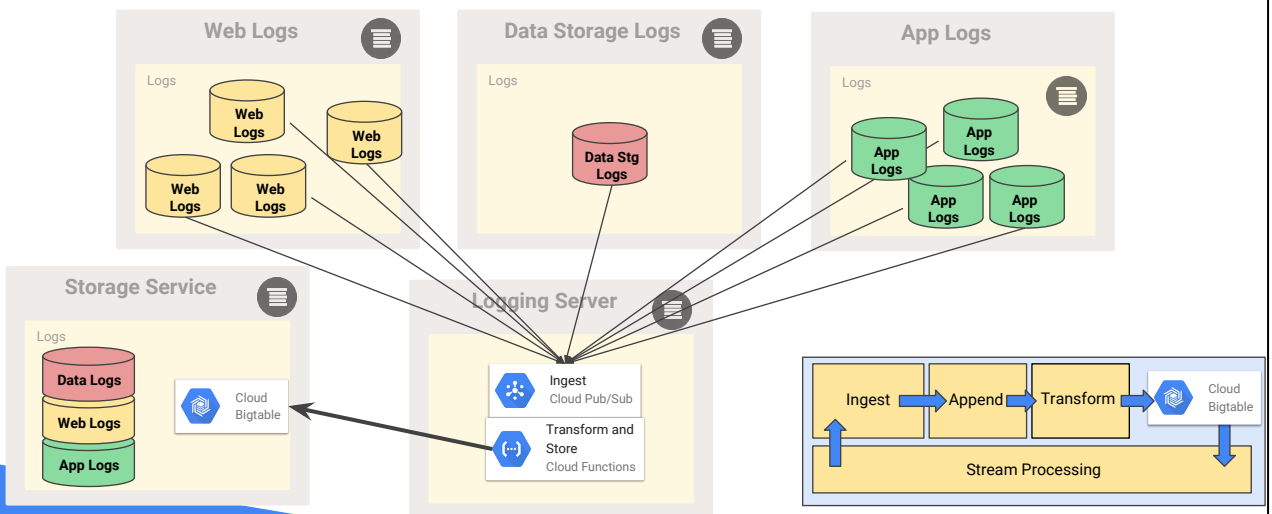
Defense in depth

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Google Cloud Training and Certification

https://pixabay.com/en/the-strategy-win-champion-1080527/

Increase security of the log files



© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Take a few minutes to design your solution

Problem: The log service has not been secured. Consider basic and more advanced methods for isolating or securing the service. Come up with three steps that you can take to increase security in the infrastructure.

Design a solution.

There are multiple designs possible depending on your assumptions. Your solution may be better than the one shown. The point of this exercise is to "think about the design" to develop your architecting skills.

You can sketch your design in a tool like http://docs.google.com/drawings

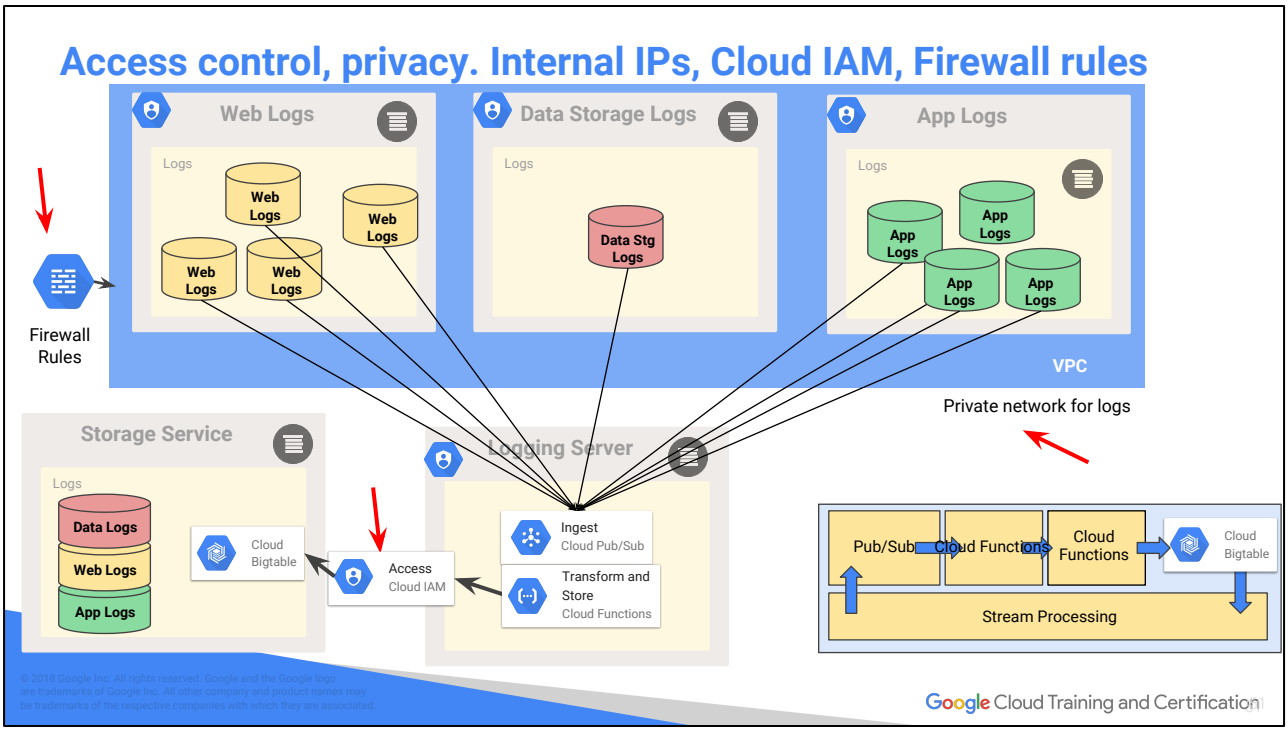
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

One solution

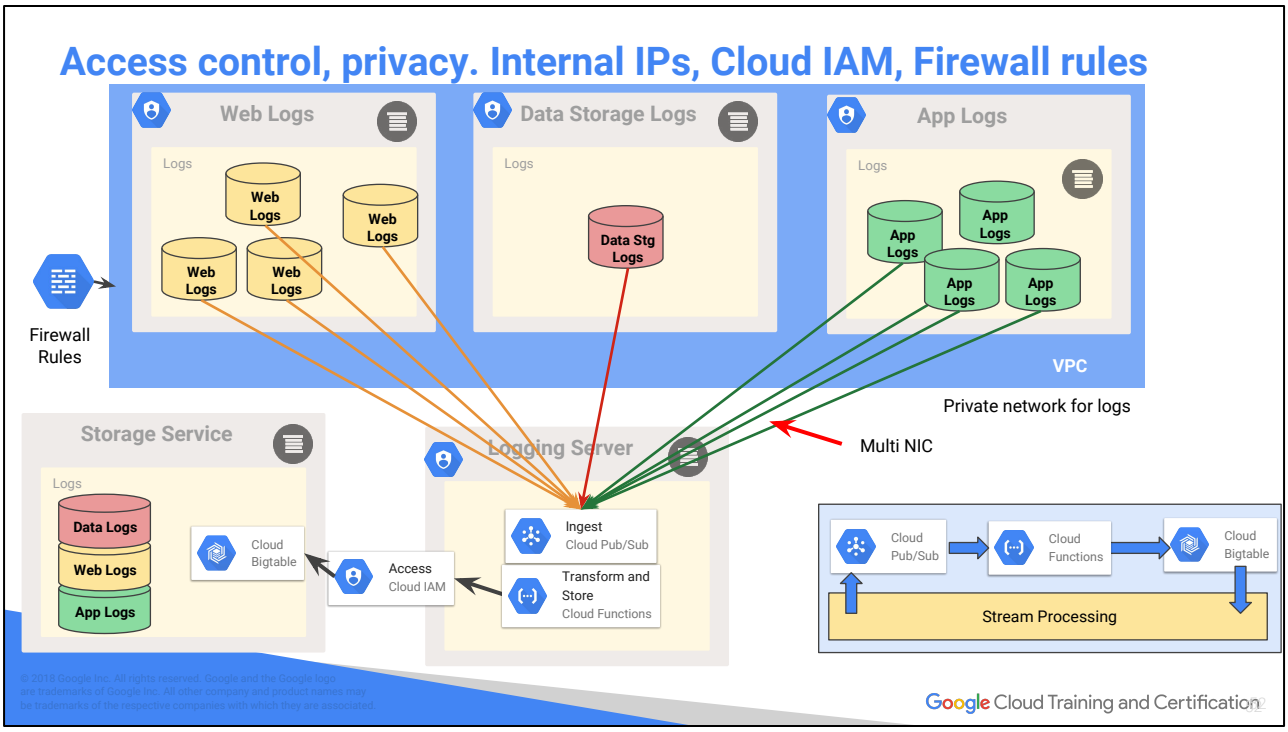
© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

Remember, there are multiple valid solutions to this challenge.

Compare your design with the example solution.
Did your design account for all the elements addressed in the example solution?



We define a VPC network expressly for logs, protected by use-case-specific firewall rules. We define IAM policies governing access to the Bigtable databases in which logs are stored.



You could also consider equipping the logging server with multiple virtual network interfaces, each handling only one type of log traffic.

Google Cloud Training and Certification

© 2018 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.