Security Considerations in GCP

Date: October 2019

Provention™

Contents

Introduction

There are two core cloud security principles that should be applied at a high-level, regardless of the cloud vendor of choice.

Least Privilege
The principal of least privilege states that people or applications have access limited to the jobs they need to perform, and nothing more. Application level access is often overlooked. API access allowing read/write can be assumed by people who can then get the same level of access used in that service account. Furthermore, there are additional risks from just relying on API keys as these are used for both identity and authentication, and any compromise can wreak havoc. A better approach is to employ OAuth 2.0 with grants and further securing with Open Id Connect for public facing APIs.

A practical approach is to always deny by default, and grant access on a need to know basis.

Defence in Depth
It is fair to assume that almost any security control can fail. This could be due to a malicious entity or a configuration oversight. With defence in depth, multiple layers of overlapping security controls are implemented so if one fails, the one below it can still protect.

GCP Security Services

Google has invested vastly, like other vendors, in securing their offering. They have designed and built their own data centres and employ multiple layers of control to satisfy their defence-in-depth physical security strategy, from securing doors, and restricting access to staff on a work requirement basis. The server boards and networking have further protection from custom-designed security chips called Titan. In terms of the shared responsibility model, Google has taken away the concern from the hardware components, leaving customers to focus on key principles to apply at the infrastructure, platform and software level.

Google provides a number of cloud services that can be utilised to secure customer data and cloud assets. In particular, there are three kinds of security services built into the Google Cloud Platform.

The first of these is **encryption**, which is triggered automatically when data is transported and is at rest.

The second is the capability to **customise controls**. For example, using your own keys and key management practices on the platform.

The third is services that are used as part of **'security by design'**.

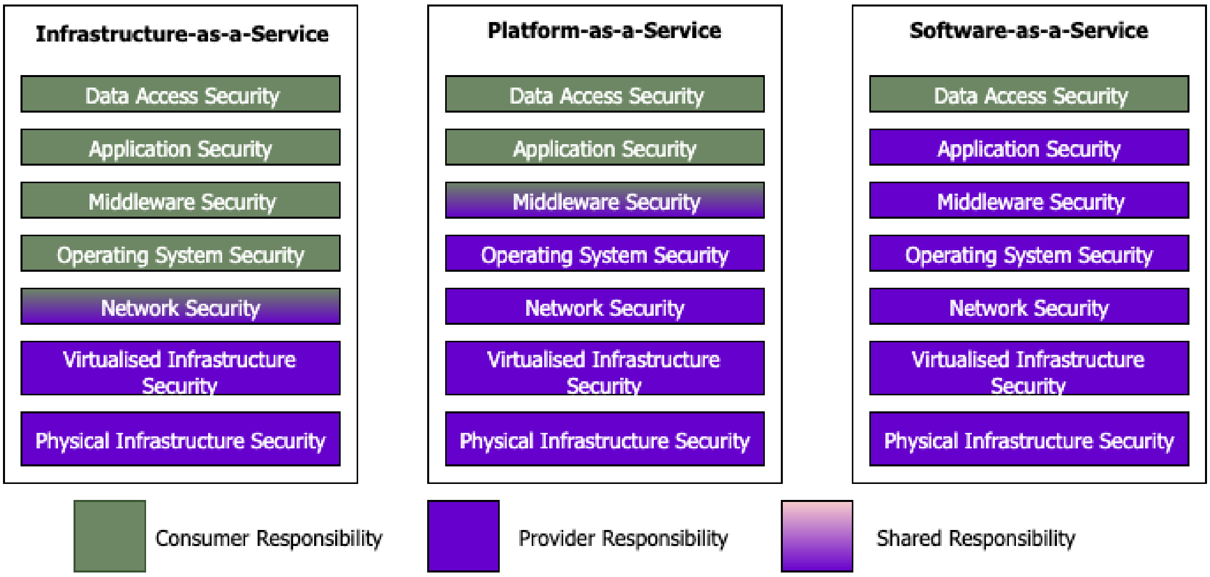
The key capabilities these three types of services cover include; network access control, firewalls, denial of service protection, resource sharing and isolation, data encryption and key management, and auditing.

Pervasive Defence in Depth

Google provides security controls that can projects can plug into. This is important to know to avoid duplication of effort, which requires an understanding of the shared responsibility model.

A generic split in the responsibility can be seen in the model below:

Cloud Shared Responsibility Model



Infrastructure-as-a-Service	Platform-as-a-Service	Software-as-a-Service
🟩 Data Access Security	🟩 Data Access Security	🟩 Data Access Security
🟩 Application Security	🟩 Application Security	🟪 Application Security
🟩 Middleware Security	▨ Middleware Security	🟪 Middleware Security
🟩 Operating System Security	🟪 Operating System Security	🟪 Operating System Security
▨ Network Security	🟪 Network Security	🟪 Network Security
🟪 Virtualised Infrastructure Security	🟪 Virtualised Infrastructure Security	🟪 Virtualised Infrastructure Security
🟪 Physical Infrastructure Security	🟪 Physical Infrastructure Security	🟪 Physical Infrastructure Security

🟩 Consumer Responsibility 🟪 Provider Responsibility ▨ Shared Responsibility

Google has complete responsibility for physical infrastructure security, which often involves controls beyond what many companies can reasonably achieve on-premise, such as biometrics access with tailgating measures, security guards and so forth.

Cloud Networking

The defence in depth principle is vastly applicable in cloud network security. A fundamental offering from Google is a Virtual Private Cloud (VPC), as they completely isolate a network. A VPC minimises exposure to the internet and allows segregation of environments. To add a further layer GCP supports third-party virtual appliances which are virtual machines running security audited applications that a customer can install. Finally, there are Google Load Balancers with hardened security controls.

Customer Security Controls

Network Controls

Customers can have a significant amount of impact of network controls with the use of GCP network access controls and firewalls. They can set up their own rules on firewalls as a first line of defence. These rules can be applied to ingress and egress traffic in order to isolate virtual machines in both directions. This enables virtual machines to talk privately to other virtual machines on the same network.

The Google Cloud Firewall is a virtual entity, aligning with its Software Defined Networking model, so the rules are applied traffic at network layer, as soon as it enters the Google platform.

It is best practice to place the firewall behind a Google Network Load Balancer. This way it can effectively block everything from the outside internet and only allow internal hosts and networks that are explicitly allowed via firewall rules.

Denial of Service Protection

Some protection relating to denial of service is built into the cloud infrastructure. There are services that adapt to demand such as autoscaling, and as Google employs a Software Defined Network (SDN) there are no hardware interfaces that can be overloaded. Additional built-in controls can be leveraged by the use of load balancers that are not transparent to customers, but are based around continuous monitoring, quotas and limits.

Another method used, at the edge, is with the use of a Cloud CDN. A CDN protects and maximises available bandwidth. This done through caching content at many points of present locations at the edge. In order to maximise the benefits, a global load balancer can be used alongside. The load balancers will drop all UDP floods and SYN floods which can exhaust the TCP connections pool.

Another layer of control can be provided by VM Traffic Throttling. This allows 10 gigs of throughput per VM for ingress, along with built in protections using quotas and limits.

Infrastructure Protection

There will be situations where the attack will need to be absorbed. To facilitate this, scaling up by adding more resources can reduce the impact. Alternatively, traffic can be split between regions with the use of a global load balancer. This way an attack originating in Asia whilst based in the UK, can be handled by spinning up a region in Asia to absorb the traffic.

Sharing and Isolation

By decoupling resource dependencies, fault-tolerant communication channels can be implemented between inter-related parts. This is useful in the design using multiple failure domains, which provides better isolation and resiliency. GCP provides several features to help in designing this approach. An effective way of isolation is through using a microservices architecture. Microservices do not communicate with other services as they have no concept of downstream or upstream services. This can be achieved using a VPC. VPCs have their own private IP space and their own IAM policies. Further isolation can be achieved using more traditional methods such as VPN tunnelling, that provides encrypted links between two or more projects.

Careful consideration and naming convention in defining Organisations, folders and projects can make this task maintainable.

Encryption

Google automatically encrypts data in motion and data at rest. Alternatively, Google provides a key management service for use with customer provided keys.

Google's server-side encryption can meet most use-cases. Especially, as remote web connections are already connected over HTTPS. A further use of HTTPS load balancer provides encryption in communication channels between cloud services and applications. Google store these keys 'in memory' so nothing is stored on the applications.

Occasionally, a customer may want greater control over encryption and the key management process. This is common in high-security environments, where Google holding the keys is not desirable. Google offers customer-managed encryption key services for such situations.

Blended Controls

The focus here is based on control, visibility and security solutions. Starting with control, IAM is the foundation of all GCP security. Best practice is to create groups and place users within the groups. This greatly simplifies the administration and maintainability of the policies. Creating folders based on organisational structures. This makes it easier to identify and following this naming convention makes it simpler to look through logs to identify resources.

It is bad practice to assign to many roles to service accounts. Service accounts can also inherit roles from groups, so it is imperative that these accounts are audited.

A better option is to limit the service accounts own roles and permissions to specific resources and tasks. It is better to create more specific service accounts than to continually keep empowering an existing account with more functions and roles.

There are several tools that can be leveraged for visibility. Tools such as logs, Stackdriver and Forseti, can discover who or what service accounts can access resources and with what permissions.

Visibility into the underlying permissions matrix is imperative in order to understand what is going on and who is doing what.

Stackdriver for logging and monitoring are sufficient for the infrastructure level visibility. For containers and microservices Istio integrated with Stackdriver will be a better option.

A point to note is GCP logging remains within the projects they are created in. This can be problematic for large organisations with 100s of projects. Stackdriver has a log aggregation export feature to accommodate this. It allows collation of logs from multiple projects across the organisation into a single log. The logs can also be filtered and transformed before sending them to either, BigQuery for analysis, Cloud Storage for long term archiving, or to Pub/Sub for integration with other third-party services.

Security solutions for remote access is a core requirement in a good security architecture. To alleviate this there are three security components that form part of a compound security solution:

- Cloud Armor for edge protection
- Identity Aware Proxy for identity management
- VPC for global reach using Google's private network

Cloud Armor at the edge of the network intercepts all incoming connection requests from remote users to internal Google hosted applications and using a simple whitelist/blacklist it determines IP addresses which are accepted onto the network. The second step is that the connection is established with the global HTTPS load balancer that will forward the request to the application. At this step the load balancer checks the user's identity using the identity-aware proxy and it considers the users profile such as the groups, roles and permissions that they are entitled to. It also checks the user's job function is compatible with the application or resource that they are requesting access to.

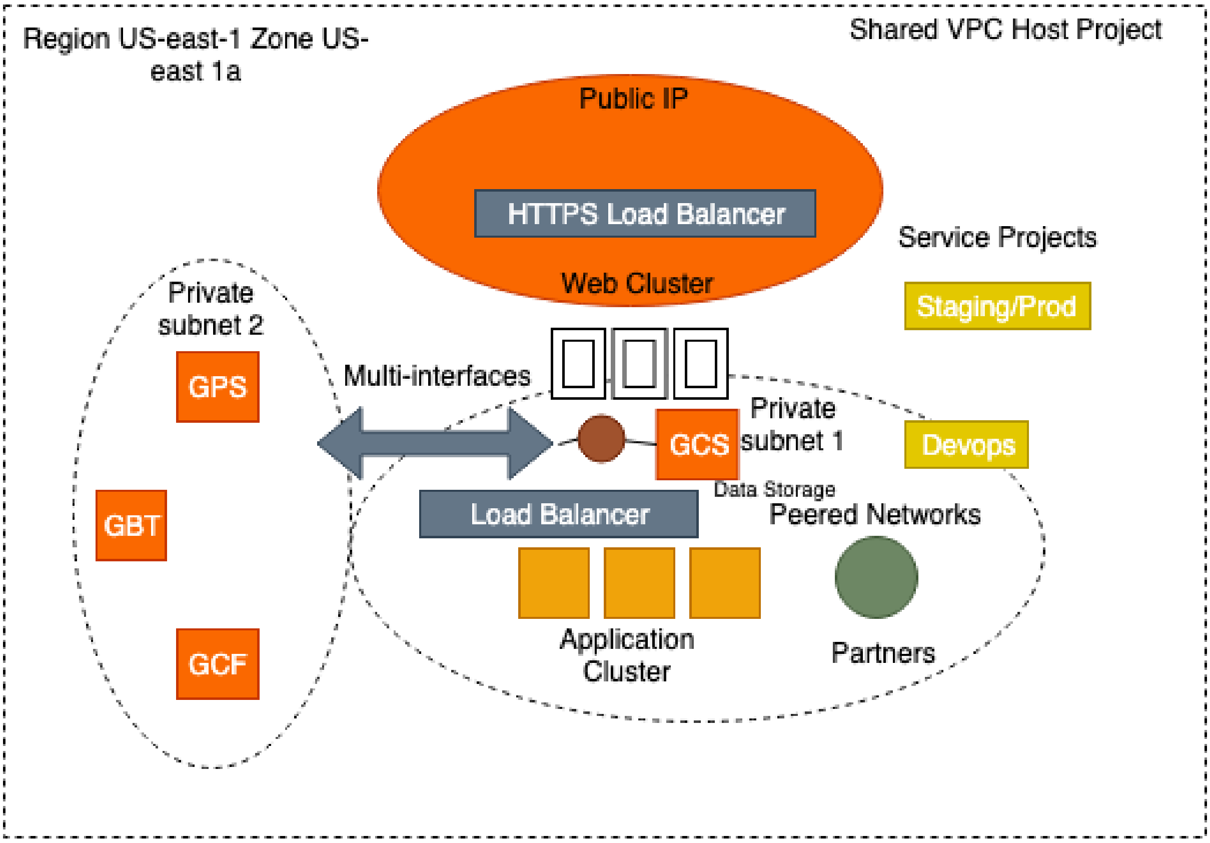
The proxy is not confined to using IAM. It can also check network identity through Active Directory Federations, LDAP, or two-factor methods as these can all be integrated with the Identity Manager.

Cloud Security Scanner

Cloud Security Scanner is a web security scanner that comes with GCP at no additional cost and is used to detect common vulnerabilities in App Engine, Compute Engine, and Google Kubernetes Engine applications. It automatically scans and detects the most common system vulnerabilities, such as cross-site scripting (XSS), flash injection, mixed content (HTTP in HTTPS) and insecure libraries.

Cloud Security Scanner can be setup, run, scheduled, and manage security scans quickly to identify and remediate well-known vulnerabilities with low false-positive rates.

Use Case



Use case provided by Alisdair Gilchrist

In this use case, we want to conduct a security audit of the functional services to identify any potential vulnerabilities as well as define the protections already in place. We also want to lock down IAM and resource management techniques such as folders and projects to limit access to the infrastructure. The Production and Staging internal teams need access as do third parties but the external partners should not have access to other internal project teams.

There are many risk mitigation controls provided by GCP, by default, so we should identify them before considering any additional security design changes.

When trying to identify any security vulnerabilities, we start by auditing our existing architecture. To do this we could use the Cloud Security Scanner to surface known vulnerabilities then work through those identified to remediate any issues. However, some security vulnerabilities may be due to design flaws which will need addressing too.

Identifying any issues with the front-end security is a good start, so locking down the external facing webservers would be the first step. There are some security techniques already deployed, by default, such as firewall and its rules when the webserver was created. There is also built-in network protection from the global load balancers as they protect against large denial of service attacks. We could bolster DoS security further by adding Cloud CDN and Cloud DNS to the design, but we will also need to consider implementing autoscaling for the front-end cluster to absorb the attack by adding additional servers.

Unauthorised access to sensitive information can be prevented by the use of VPCs, and a private IP subnet range. This prevents a hacker getting inside, directly, from the internet. The first layer of defence must be to prevent unauthorised access to the public facing webservers, by isolating the upload webservers by using private IP addressing on the internal interfaces. By giving them private IPs means that if the web servers need to talk to the back-end services, they can use a secondary NIC in the same private network as the back-end servers. This means the GCS and CBT is accessed over the private network.

Working through the controls, we have added firewalls, and firewall rules to restrict access to certain ports. We have also addressed denial of service (DoS) risk by making the design more scalable and reliable by adding autoscaling to the front-end group. We have also restricted access to the back-end servers by giving them private addresses which are inaccessible from the internet. They can only be accessed from the front-end servers' secondary interface that resides in the private address space. Additionally, the design is now in separate zones that can be isolated against fault tolerances, complimented with security accounts managed by IAM. Access to the Production, Development, and the Staging teams through a shared VPC via a designated host project and sharing its subnet with the Production and Staging project teams as service projects, along with the DevOps team that utilises a different folder.

We can further lock down access by placing both the Production and Staging service projects in a common folder and assigning IAM permissions to that folder. This will allow both the Production and Staging project teams to communicate with all the resources in the host VPC. The DevOps project team will remain in their own folder for better granular control of IAM permissions.

For external partners, rather than sharing the VPC, we can peer with the partner network to establish a connection so that they can communicate without a VPN using private addressing. Using a peered VPC ensures the partner project have access to the peered VPN and not to internal Production, DevOps, or the Staging projects.

We could then further lock down remote administration access via a bastion host to limit administrative access.

Conclusion

Although organisations have or are planning to move to a cloud environment like AWS, Azure or GCP, many are still at a loss when considering securing their cloud environment. The key objective of cloud security is keeping the data secure in the Cloud. According to Gartner, organisations should never assume a Cloud service automatically means that whatever they do with the environment will be secure.

If your organisation is planning to move to the Cloud, or has done so already, it is crucial to keep security in mind throughout the migration project.

Organisations can no longer assume that whatever they store in the Cloud is automatically secure. Review the shared responsibility model to understand what customer's responsibility is and what is covered by the Cloud provider. Additionally, conduct a thorough planning, evaluation and monitoring before, during and after the Cloud migration.

Provention specialises in Cloud Security and provide architecture, engineering and maturity assessment services for organisations looking for support with redesign, uplift or strategic guidance.

Our expertise cover, but not limited to; Microsoft Azure, AWS, GCP, OpenStack, IBM, and Kubernetes and Docker containerisation. We have assisted organisations with FedRAMP, PCI DSS, and GDPR compliance needs with a structured approach.

Provention™
The Mansion
Sherwood Drive
Bletchley
MK3 6EB

Tel: 01908 787783
info@provention.co.uk

www.provention.co.uk