

# Caso de Estudio: Arquitectura de Red Segura y Modelo Zero Trust en Google Cloud

**Consultor:** Christhian Alberto Rodríguez García

**Fecha:** Noviembre 2025

**Tecnologías:** Google Cloud Platform (GCP), VPC, Firewall, Identity-Aware Proxy (IAP), Compute Engine.

**Certificación Obtenida:** Build a Secure Google Cloud Network Skill Badge.

## 1. Resumen Ejecutivo

En este proyecto, asumí el rol de Consultor de Seguridad para "Juice Shop", una empresa emergente cuya infraestructura en la nube presentaba vulnerabilidades críticas debido a una configuración inicial insegura.

El objetivo fue rediseñar la arquitectura de seguridad perimetral e interna implementando un modelo de **Defensa en Profundidad**. Se logró eliminar la exposición de puertos de administración a internet pública, implementando accesos verificados por identidad (IAP) y segmentación de red interna, todo esto sin interrumpir el servicio web público.

## 2. El Desafío: Situación Inicial

La auditoría inicial de la infraestructura reveló graves fallos de seguridad (Antipatrones):

- **Reglas permisivas:** Existían reglas de firewall (`open-access`) que permitían tráfico desde `0.0.0.0/0` a todos los puertos.
- **Superficie de ataque expuesta:** Los servidores de administración (Bastion) y de aplicaciones tenían IPs públicas expuestas con puertos SSH abiertos, vulnerables a ataques de fuerza bruta.
- **Falta de segmentación:** No existía control de tráfico entre las subredes internas.

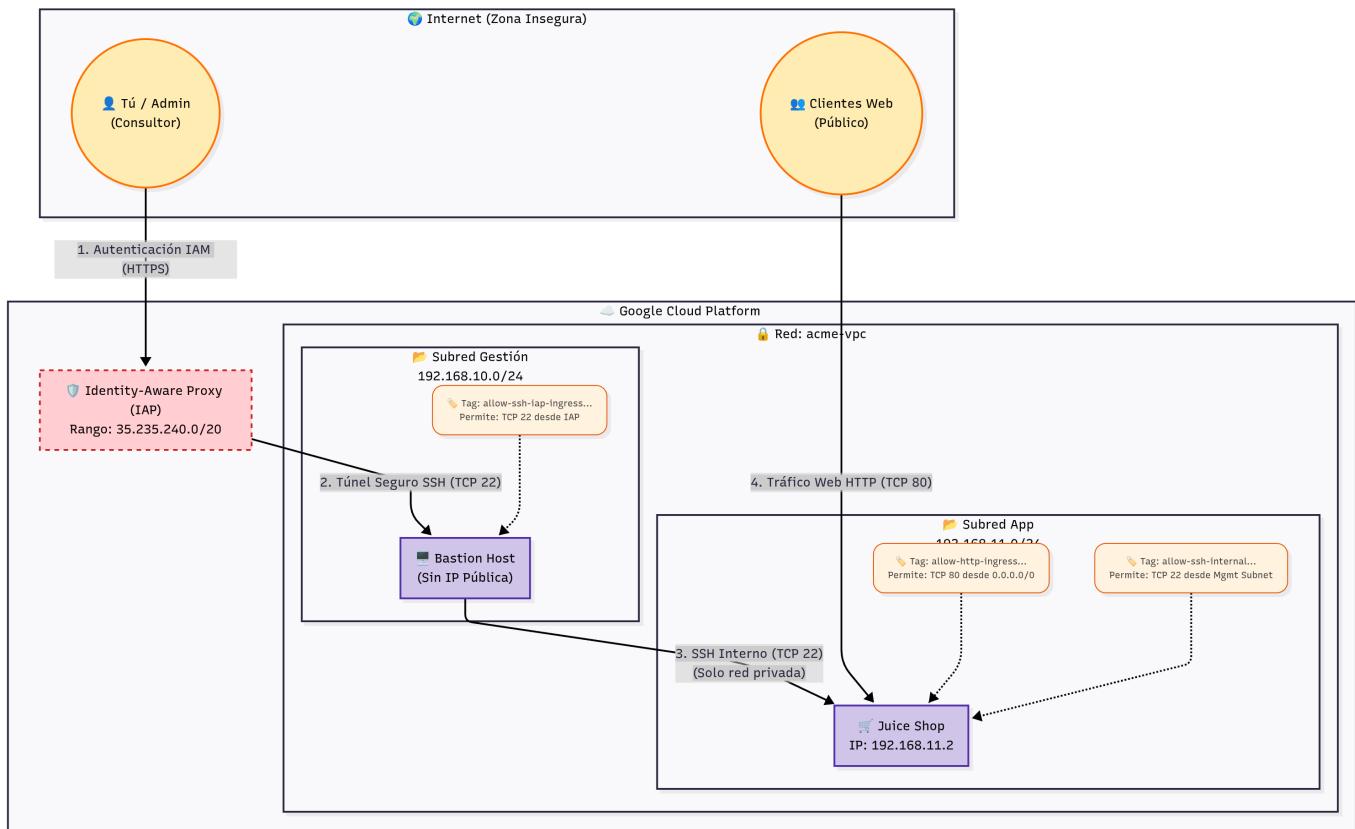
## 3. Estrategia de Solución: Arquitectura Zero Trust

Para mitigar estos riesgos, diseñé una solución basada en tres pilares fundamentales de ciberseguridad:

- 1. Principio de Mínimo Privilegio (PoLP):** Solo permitir el tráfico estrictamente necesario.
- 2. Identity-Aware Proxy (IAP):** Reemplazar el acceso SSH tradicional por túneles TCP encapsulados en HTTPS, autenticados por Google IAM.
- 3. Micro-segmentación con Etiquetas:** Uso de *Network Tags* para aplicar reglas de firewall granulares a instancias específicas, no a toda la red.

## 4. Implementación Técnica

### Esquema



### Fase 1: Hardening (Endurecimiento de la Red)

El primer paso crítico fue la eliminación de la deuda técnica de seguridad. Se identificaron y eliminaron las reglas de firewall heredadas que permitían el acceso irrestringido. Esto colocó a la red en un estado de "Denegación por defecto".

*Fig 1. Panel de Firewall tras la limpieza. Se eliminaron reglas peligrosas y se observa una configuración limpia y específica.*

#### VPC firewall rules

Firewall rules control incoming and outgoing traffic to an instance. By default, all incoming traffic to your network is blocked. [Learn more](#)

Note: App Engine firewalls are managed in the [App Engine Firewall rules section](#)

The screenshot shows the Google Cloud VPC Firewall Rules interface. At the top, there's a note about SMTP port 25 being disallowed. Below that are refresh, log configuration, and delete buttons. A filter bar allows entering a property name or value. The main table lists six firewall rules:

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs
<a href="#">open-access</a>	Ingress	Apply to all	IP ranges:	tcp	Allow	1000	<a href="#">acme-vpc</a>	Off
<a href="#">default-allow-icmp</a>	Ingress	Apply to all	IP ranges:	icmp	Allow	65534	<a href="#">default</a>	Off
<a href="#">default-allow-internal</a>	Ingress	Apply to all	IP ranges:	tcp:0-65535 udp:0-65535 icmp	Allow	65534	<a href="#">default</a>	Off
<a href="#">default-allow-rdp</a>	Ingress	Apply to all	IP ranges:	tcp:3389	Allow	65534	<a href="#">default</a>	Off
<a href="#">default-allow-ssh</a>	Ingress	Apply to all	IP ranges:	tcp:22	Allow	65534	<a href="#">default</a>	Off

## Fase 2: Acceso Administrativo Seguro (Bastion Host + IAP)

En lugar de asignar una IP pública al servidor Bastion, configuré el acceso exclusivamente a través del **Identity-Aware Proxy**.

- Configuración:** Se creó una regla de firewall permitiendo tráfico al puerto 22 únicamente desde el rango de IP de infraestructura de Google: 35.235.240.0/20
- Resultado:** El servidor es invisible para los escáneres de puertos en internet, pero accesible para los administradores autenticados.

## Fase 3: Publicación Segura de Aplicaciones

Para el servidor web juice-shop, se habilitó el tráfico HTTP (Puerto 80) desde internet (0.0.0.0/0). Sin embargo, para evitar movimientos laterales, esta regla se asoció estrictamente a la etiqueta de red de la instancia web.

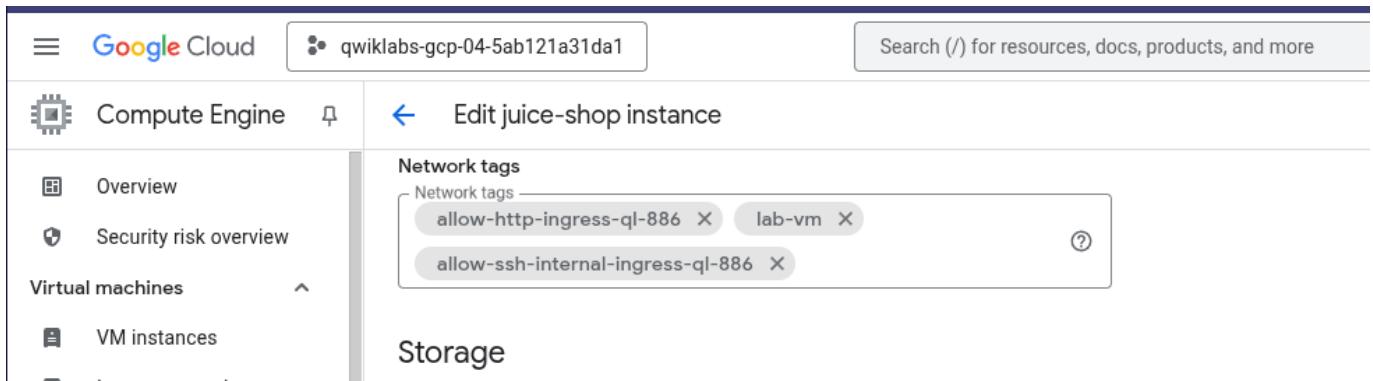


Fig 2. Detalle de la instancia 'juice-shop'. Se observan las etiquetas de red (Network Tags) que vinculan la instancia con las reglas de firewall específicas, aislando su función.

## Fase 4: Segmentación de Tráfico Interno

El servidor de aplicaciones no debe recibir conexiones SSH desde internet. Su administración se restringió exclusivamente al tráfico proveniente de la subred de gestión donde reside el Bastion Host.

Análisis de Subred:

Se identificó el rango CIDR de la subred de gestión (acme-mgmt-subnet) para crear una regla de ingreso precisa.

Private Google Access is in effect (even though it has not been enabled manually) when Cloud NAT is enabled for the primary IP range of the subnetwork.

[Learn more](#)

Name	Region	Stack Type	Primary IPv4 range	Secondary IPv4 ranges	IPv6 ranges
acme-app-subnet	us-west1	IPv4 (single-stack)	192.168.11.0/24		
acme-mgmt-subnet	us-west1	IPv4 (single-stack)	192.168.10.0/24		

Reserved proxy-only subnets for load balancing

Name	Region	IP address ranges	Gateway	Role	Purpose
No rows to display					

[Equivalent REST](#)

Fig 3. Identificación del rango de IP interno (192.168.10.0/24) para permitir el tráfico seguro entre el Bastion y la Aplicación.

## 5. Validación y Pruebas de Conectividad

Para certificar la seguridad de la arquitectura, se realizó una prueba de conexión de "doble salto" (Double-hop SSH).

### Flujo de la prueba:

1. Conexión desde mi estación de trabajo local hacia el **Bastion** mediante el túnel IAP (autenticado por IAM).
2. Conexión SSH interna desde el Bastion hacia la IP privada de **Juice Shop** (192.168.11.2).

VM instances    [Create instance](#)    [Import VM](#)    [Refresh](#)

[Instances](#)    [Observability](#)    [Instance schedules](#)

VM instances

[Filter](#) Enter property name or value

Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	<a href="#">bastion</a>	us-west1-a			192.168.10.2 ( <a href="#">nic0</a> )		<a href="#">SSH</a> <a href="#">⋮</a>
<input checked="" type="checkbox"/>	<a href="#">juice-shop</a>	us-west1-a			192.168.11.2 ( <a href="#">nic0</a> )	35.197.16.107 ( <a href="#">nic0</a> )	<a href="#">SSH</a> <a href="#">⋮</a>

Related actions

```

ssh.cloud.google.com/v2/ssh/projects/qwiklabs-gcp-04-5ab121a31da1/zones/us-west1-a/instances/bastion?authuser=0&hl=en_US
ssh.cloud.google.com/v2/ssh/projects/qwiklabs-gcp-04-5ab121a31da1/zones/us-west1-a/instances/bastion
SSH-in-browser
Linux bastion 5.10.0-36-cloud-amd64 #1 SMP Debian 5.10.244-1 (2025-09-29) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/student-02-af3723c6f787'.
student-02-af3723c6f787@bastion:~$ ssh 192.168.11.2
The authenticity of host '192.168.11.2 (192.168.11.2)' can't be established.
ECDSA key fingerprint is SHA256:ez2bL4dCFXgnkjemRumiq15m0zp13zwUeNbIWzI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.11.2' (ECDSA) to the list of known hosts.
Linux juice-shop 5.10.0-36-cloud-amd64 #1 SMP Debian 5.10.244-1 (2025-09-29) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Creating directory '/home/student-02-af3723c6f787'.
student-02-af3723c6f787@juice-shop:~$ 

```

Fig 4. Evidencia de la terminal ("Money Shot"). Muestra la conexión exitosa al Bastion y el posterior salto a la instancia interna 'juice-shop' utilizando direcciones IP privadas, confirmando el aislamiento de la red.

## 6. Conclusión

La implementación fue exitosa, logrando una arquitectura de 3 capas segura y funcional. La superficie de ataque se redujo drásticamente al eliminar puntos de entrada públicos innecesarios.

### Habilidades Demostradas:

- Configuración avanzada de VPC Firewall Rules.
- Implementación de Seguridad Zero Trust con Google IAP.
- Gestión de Compute Engine y Network Tags.
- Troubleshooting de conectividad de red.