

Práctica 3

Primera solución

Las máquinas virtuales usadas en este caso son las siguientes:

VM instances

CREATE INSTANCEIMPORT VMREFRESHSTART / RESUMESTOPSUSPENDOPERATE

INSTANCES

INSTANCE SCHEDULES

VM instances are highly configurable virtual machines for running workloads on Google infrastructure. [Learn more](#)

Filter

Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	✓	msalto	us-central1-a			10.128.0.3 (nic0)	34.121.37.7 (nic0)	SSH ⌵ ⋮
<input type="checkbox"/>	✓	servidorweb	us-central1-a			10.128.0.2 (nic0)	34.173.225.157 (nic0)	SSH ⌵ ⋮

Se muestra cómo se accede a la primera máquina de salto mediante SSH usando la IP pública de dicha máquina de salto, una vez dentro de la máquina de salto se accede usando de nuevo SSH, pero esta vez entre las máquinas que están en la misma red, de forma que se hace SSH al servidor web usando la IP privada.

```
jorge@jorge-virtual-machine:~$ ssh 34.121.37.7
Linux msalto 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) 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.
Last login: Fri Sep 16 06:55:06 2022 from 130.206.68.4
jorge@msalto:~$ ssh 10.128.0.2
Linux servidorweb 5.10.0-17-cloud-amd64 #1 SMP Debian 5.10.136-1 (2022-08-13) 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.
Last login: Fri Sep 16 06:55:22 2022 from 10.128.0.3
jorge@servidorweb:~$
```

Dentro del servidor web se ha modificado la página web a la cual se accede por el puerto 80 usando http.

← → ↺

34.121.116.6

Funcionamiento de la maquina de salto y servidor web

Los firewalls rules usados para esta solución han sido las siguientes:

Firewall

CREATE FIREWALL POLICY

CREATE FIREWALL RULE

Easy to deploy network threat detection with Google Cloud IDS. [Learn more](#)

VPC firewall rules

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

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

SMTP port 25 disallowed in this project

REFRESH

CONFIGURE LOGS

DELETE

Filter

Enter property name or value

	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last hit	Insights
<input type="checkbox"/>	serverpuerto80	Ingress	serverpuerto80	IP ranges: 0.0.0.0/0	tcp:80	Allow	1000	default	Off	—	—	
<input type="checkbox"/>	sshextern	Ingress	sshextern	IP ranges: 130.206.68.4	tcp:22	Allow	1000	default	Off	—	—	
<input type="checkbox"/>	sshintern	Ingress	sshintern	IP ranges: 10.128.0.3	tcp:22	Allow	1000	default	Off	—	—	

Por último, estos firewalls rules han sido asignados a las máquinas virtuales mediante los tags:

← servidorweb

EDIT

RESET

CREATE MACHINE IMAGE

CREATE SIMILAR

START / RESUME

STOP

SUSPEND

OPERATE

DETAILS

OBSERVABILITY

OS INFO

SCREENSHOT

Network tags

serverpuerto80

sshintern

Network interfaces

Name	Network	Subnetwork	Primary internal IP address	Alias IP ranges	Stack Type	External IP address	Network
nic0	default	default	10.128.0.2		IPv4	34.173.225.157 (Ephemeral)	Premium

← msalto

EDIT

RESET

CREATE MACHINE IMAGE

CREATE SIMILAR

START / RESUME

STOP

SUSPEND

DELETE

OPERATE

DETAILS

OBSERVABILITY

OS INFO

SCREENSHOT

Firewalls

HTTP traffic	Off
HTTPS traffic	Off

Network tags

sshextern

Network interfaces

Name	Network	Subnetwork	Primary internal IP address	Alias IP ranges	Stack Type	External IP address	Network
nic0	default	default	10.128.0.3		IPv4	34.121.37.7 (Ephemeral)	Premium

Además, se tuvieron que generar tanto clave privado como pública en el sistema operativo donde se crean ambas máquinas (jorge-virtual machine) y en la máquina de salto.

Segunda solución

Parte 1

Eliminación IP pública del servidor web

El primer paso a realizar en esta solución es eliminar la IP pública del servidor web.

← Edit servidorweb instance

increase total egress bandwidth

Maximum outbound network bandwidth: 1Gbps

Network interfaces ⓘ

Network interface is permanent

Edit network interface

Network *

default

Subnetwork *

default IPv4 (10.128.0.0/20)

ⓘ To use IPv6, you need an IPv6 subnet range. [LEARN MORE](#)

⚠ You can change either IP Stack type or Network and Subnetwork in a single edit. Save and edit again if you need to change both settings.

IP stack type

☒ IPv4 (single-stack)

☐ IPv4 and IPv6 (dual-stack)

Primary internal IP

Ephemeral (Custom)

Custom ephemeral IP address *

10.128.0.2

Alias IP ranges

+ ADD IP RANGE

External IPv4 address

None

<input type="checkbox"/>	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Connect
<input type="checkbox"/>	✓	msalto	us-central1-a			10.128.0.3 (nic0)	34.172.166.252 (nic0)	SSH ▾ ⋮
<input type="checkbox"/>	✓	servidorweb	us-central1-a			10.128.0.2 (nic0)		SSH ▾ ⋮

El servidor por lo tanto no se puede conectar a internet como se puede ver en la siguiente imagen:

```
jorge@servidorweb:~$ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  nginx
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 92.9 kB of archives.
After this operation, 104 kB of additional disk space will be used.
Err:1 http://deb.debian.org/debian bullseye/main amd64 nginx all 1.18.0-6.1+deb11u2
  Could not connect to debian.map.fastlydns.net:80 (199.232.30.132), connection timed out Unable to connect to deb.debian.org:http:
  Failed to fetch http://deb.debian.org/debian/pool/main/n/nginx/nginx_1.18.0-6.1%2bdeb11u2_all.deb Could not connect to debian.map.fastlydns.net:80 (199.232.30.132), connection timed out Unable to connect to deb.debian.org:http:
  Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

Creación de NAT

Se introduce un NAT para poder acceder a Internet y así poder instalar correctamente nginx. Como se ve en la segunda imagen, nginx ya se puede instalar sin problema:

Cloud NAT

CREATE CLOUD NAT GATEWAY

DELETE

REFRESH

Easy to deploy network threat detection with Google Cloud IDS. [Learn more](#)

Filter Enter property name or value

<input type="checkbox"/>	Gateway name ↑	Region	Cloud router	Status	
<input type="checkbox"/>	natgateway	us-central1	routernat	Running	⋮

```
jorge@servidorweb: $ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  nginx
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 92.9 kB of archives.
After this operation, 104 kB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bullseye/main amd64 nginx all 1.18.0-6.1+deb11u2 [92.9 kB]
Fetched 92.9 kB in 0s (1841 kB/s)
perl: warning: Setting locale failed.
perl: warning: Please check that your locale settings:
    LANGUAGE = (unset),
    LC_ALL = (unset),
    LC_TIME = "es_ES.UTF-8",
    LC_MONETARY = "es_ES.UTF-8",
    LC_ADDRESS = "es_ES.UTF-8",
    LC_TELEPHONE = "es_ES.UTF-8",
    LC_NAME = "es_ES.UTF-8",
    LC_MEASUREMENT = "es_ES.UTF-8",
    LC_IDENTIFICATION = "es_ES.UTF-8",
    LC_NUMERIC = "es_ES.UTF-8",
    LC_PAPER = "es_ES.UTF-8",
    LANG = "C.UTF-8"
are supported and installed on your system.
perl: warning: Falling back to a fallback locale ("C.UTF-8").
Selecting previously unselected package nginx.
(Reading database ... 54064 files and directories currently installed.)
Preparing to unpack .../nginx_1.18.0-6.1+deb11u2_all.deb ...
Unpacking nginx (1.18.0-6.1+deb11u2) ...
Setting up nginx (1.18.0-6.1+deb11u2) ...
```

Creación de Load Balancer

El siguiente paso es crear un servicio backend, para luego usarlo en el load balancer. El servicio backend necesita la creación de un Network endpoint group y un health checker para que funcione correctamente.

Network endpoint group

Network endpoint group details

DELETE

networkendpointgroup

Network endpoints	1
Network endpoint group type	Network Endpoint Group (Zonal)
Scope	Zonal (us-central1-a)
Subnet	default
Default port	80
In use by	backendservice
Creation time	2022-09-18T01:39:17.327-07:00

Network endpoints in this group

Network endpoints represent your services (applications, load balancing) and diverse infrastructure (VM instances, containers etc) in a standard manner regardless of their location. [Learn more](#)

ADD NETWORK ENDPOINT

REMOVE ENDPOINT

Filter Filter by instance, ip or port

☐

IP Address

Health status

Port

Host vm

☐

10.128.0.2

80

servidorweb

⋮

EQUIVALENT REST

Health Checks

Name
healthcheckbackend

Description

Protocol TCP Port * 80

Proxy protocol PROXY_V1

Request ? Response ?

Logs
☐ On
Turning on Health check logs can increase costs in Cloud Logging.
☒ Off

Health criteria
Define how health is determined: how often to check, how long to wait for a response, and how many successful or failed attempts are decisive

Check interval * 5 seconds ? Timeout * 5 seconds ?

Healthy threshold * 2 consecutive successes ?

Unhealthy threshold * 2 consecutive failures ?

Estos elementos creados se añaden a la hora de configurar el backend del load balancer.

Create backend service

Name *
backendservice ?
Lowercase, no spaces.

Description

Backend type
Zonal network endpoint group

Protocol HTTP ? Named port http ?

Timeout * 30 seconds ?

Backends

Regions
us-central1

New backend ^

Network endpoint group * networkendpointgroup

Balancing mode ?
Rate

Maximum RPS * 10 RPS ? Scope per endpoint

Capacity * 100 % ?

CANCEL DONE

CREATE CANCEL

Tras crear el servicio backend hay que crear un certificado, que también será usado en el load balancer. Para poder así permitir el HTTPS con un certificado que ha sido creado por nosotros..

Creación del certificado

```
jorge@jorge-virtual-machine: /home/pract$ sudo nano KEY.key
[sudo] password for jorge:
jorge@jorge-virtual-machine: /home/pract$ openssl req -x509 -newkey rsa:2048 -keyout KEY.key -out cert.pem -days 365 -nodes
+++++
.....
+++++
req: Can't open "KEY.key" for writing, Permission denied
jorge@jorge-virtual-machine: /home/pract$ sudo openssl req -x509 -newkey rsa:2048 -keyout KEY.key -out cert.pem -days 365 -nodes
+++++
.....
+++++
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
or some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:MADRID
Locality Name (eg, city) []:MADRID
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ICAI
Organizational Unit Name (eg, section) []:ASR
Common Name (e.g. server FQDN or YOUR name) []:JORGE
Email Address []:
```

Create a Certificate

Name *

certweb

Lowercase, no spaces.

Description

Create mode

☒ Upload my certificate

Use your own public key certificate, certificate chain and private key

☐ Create Google-managed certificate

Google will automatically provision an SSL certificate once you finish your LB configuration and point DNS of all domains specified to the IP associated with the Load Balancer

Certificate *

/k4NVRm9X8k6QcyWFIZX1
jxNyD8kVAmqdz2H6Ug==
-----END CERTIFICATE-----

UPLOAD

Private Key *

/7LuEs88E+rzqwkoDFifPH1
KbTqYQRcUsr6BJ5p6T7JXTM=
-----END PRIVATE KEY-----

UPLOAD

DNS Hostnames

JORGE

Expires

✓

Sep 18, 2023, 10:58:49 AM

Serial number

34:70:69:C:89:04:14:DC:BE:57:1
0:5C:88:5B:90:4A:B3:73:D1:4B

Certificate Issuer

JORGE

CREATE

CANCEL

Al crear el load balancer (en el frontend) hay que tener en cuenta que se va a realizar el HTTP offloading. Por lo tanto, se a habilitar la última opción que permite al load balancer devolver https cuando recibe un request http.

Frontend Configuration

Name
loadbalancerredirect ⓘ
Lowercase, no spaces.

▼ **DESCRIPTION**

Protocol
HTTPS (includes HTTP/2) ▼
Select HTTPS to support clients that support HTTP/2. The load balancer automatically offers HTTP/2 as part of the TLS handshake.

Network Service Tier
Premium
Global HTTP(S) load balancing only supports the Premium Network Service tier. [More information](#)

IP version
IPv4 ▼

IP address
ipestatica ▼

Port
443 ▼
Global HTTPS load balancing only supports TCP port 443. [More information](#)

Certificate *
certweb ⓘ ▼

▼ **ADDITIONAL CERTIFICATES**

SSL policy *
GCP default ▼

QUIC negotiation
Automatic (default) ▼

☒ Enable HTTP to HTTPS redirect

Preguntas

- ¿Qué ventajas e inconvenientes tiene hacer https offloading en el balanceador?

Ventajas

- Gracias a esto el server no necesita encriptar ni desencriptar a la información de entrada y salida al server.
- Reduce la carga del trabajo del server y ahorra la carga computacional del servidor.
- Incrementa la velocidad del server.

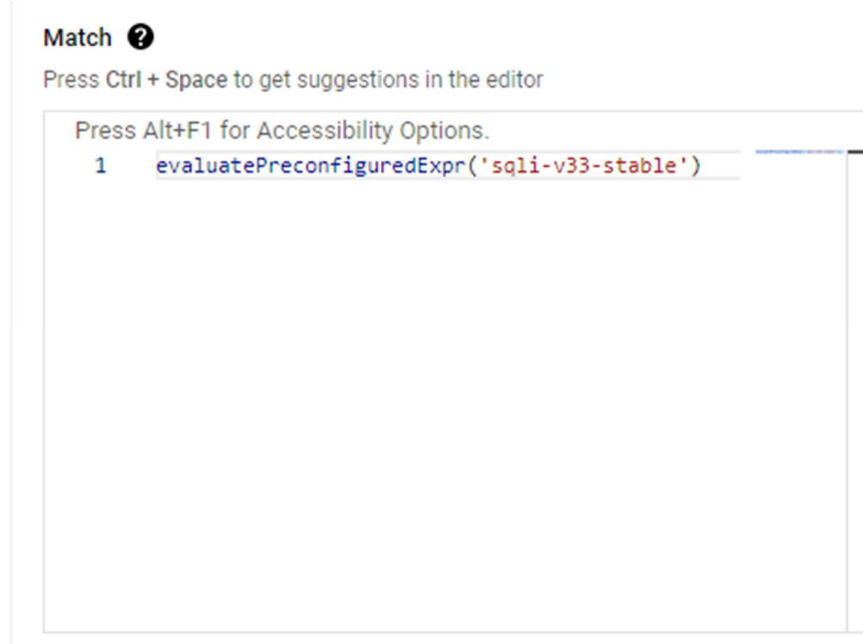
Desventajas

- La información que pasa del load balancer al servidor web esta desencriptada de forma que es vulnerable a un ataque MitM(Man in the Middle).
- El server ha de compartir la clave privada con el load balancer por lo que puede ser peligroso.
- ¿Qué pasos adicionales has tenido que hacer para que la máquina pueda salir a internet para poder instalar el servidor nginx?
Tras haber eliminado la dirección IP pública del servidor web, este no tiene acceso a internet. Por lo tanto, instalamos un NAT de salida que permita la conexión del servidor a internet. Una vez conectado se ha podido instalar nginx usando “sudo apt install nginx”, dicha instalación se ha realizado desde dentro de la máquina virtual del servidor web.

Parte 2

Para que nuestra máquina sea protegida a de ataques SQL injection, Cross Syte Scripting y el tráfico este restringido a países europeos hay que acceder a Cloud Armor donde se establecen estas políticas de seguridad.

SQL injection



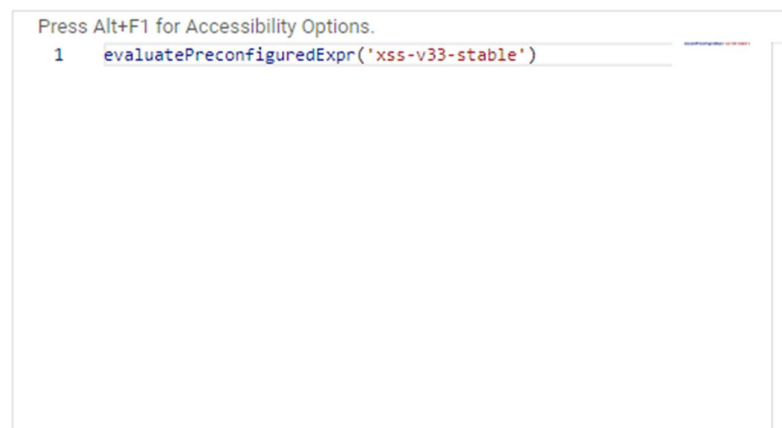
XSS Protection

Mode


- ☐ Basic mode (IP addresses/ranges only) ?
- ☒ Advanced mode ?


Match ?

Press Ctrl + Space to get suggestions in the editor



Restricción solo Europa

 Advanced mode 

Match 

Press Ctrl + Space to get suggestions in the editor

Press Alt+F1 for Accessibility Options.

```
1 '[AD,AT,BE,CH,DE,DK,EE,ES,FI,FR,GR,IT,HR,IR,GB,NL,PT]'.
  contains(origin.region_code)
```

Por lo tanto, la política de seguridad se reduce al siguiente conjunto de reglas:

securitypolicy

TypeBackend security policy

Description

Contains4 rules

Applies to0 targets





Adaptive protectionDisabled

RULESTARGETSLOGS

Rules are evaluated by priority. Lower numbers are evaluated first. [Learn more](#)

ADD RULEDELETEMORE

FilterEnter property name or value

<input type="checkbox"/>	Action	Type	Match	Description	Priority	↑
<input type="checkbox"/>	 Allow		[AD,AT,BE,CH,DE,DK,EE,ES,FI,FR,GR,IT,HR,IR,GB,NL,PT] contains(origin.region_code)	Allow Europe traffic	0	⋮
<input type="checkbox"/>	 Deny (403)		evaluatePreconfiguredExpr('sqli-v33-stable')	Sql injection	1	⋮
<input type="checkbox"/>	 Deny (403)		evaluatePreconfiguredExpr('xss-v33-stable')	XSS	2	⋮
<input type="checkbox"/>	 Deny (403)	IP addresses/ranges	*(All IP addresses)	Default rule, higher priority overrides it	2,147,483,647	⋮

Esta política se debe añadir a la configuración del backend:

Backend configuration

Create or select a backend service for incoming traffic. You can add multiple backend services and backend buckets.

Backend services & backend buckets

backendservice

Backend services

Name	Region	Instance groups/Network endpoint groups
backendservice	us-central1	1 network endpoint group

By default, Cloud CDN will cache static content - including web assets and video files - that are not explicitly marked as private for the configured default time to live (TTL), without requiring any changes at your origin.

☒ Cache static content (recommended)

☐ Use origin settings based on Cache-Control headers

☐ Force cache all content

Client time to live: 1 hour

Default time to live: 1 hour

Maximum time to live: 1 day

Cache key: Default (include all components of a request URL)

Health check: healthcheckbackend

Logging: ☐ Enable logging

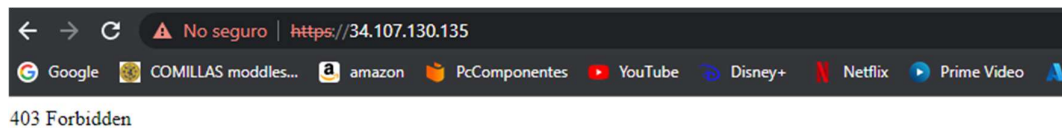
Security: Cloud Armor backend security policy

Cloud Armor edge security policy

ADVANCED CONFIGURATIONS

UPDATE CANCEL

Para comprobarlo se quita España de dentro de los países que tienen permitido acceder, entonces al intentar acceder nos da un error 403.



Cuarta Solución

¿Qué otras mejoras se te ocurrirían para mejorar la seguridad o disponibilidad del servidor web?

Para aumentar la disponibilidad del servidor web, una mejora seria dar lugar a redundancia, es decir, crear otros load balancer a través de los cuales se pueden acceder al servidor web, en caso de que uno de estos falle tener la posibilidad de conectarnos a través de otro.

Para aumentar la seguridad del servidor web es buena idea añadir más reglas a la política de seguridad que se ha configurado anteriormente. Como por ejemplo protección ante los ataques de inclusión de archivos (LFI attacks), se trata de un ataque que engaña al servidor para que ejecute y exponga archivos no deseados.