

Práctica 1

ARQUITECTURA DE SERVICIOS EN RED

RAÚL GONZÁLEZ GÓMEZ

Se crean las máquinas virtuales que se van a emplear, en este caso, una máquina que sirve como servidor web, y otra que hace de máquina intermedia para acceder al servidor web.

Se demuestra la creación de las diferentes máquinas en la siguiente captura de pantalla

Todas las direcciones Ip

IP addresses										
RESERVE EXTERNAL STATIC ADDRESS										
REFRESH										
RELEASE STATIC ADDRESS										
ALL										
INTERNAL IP ADDRESSES										
EXTERNAL IP ADDRESSES										
IPV4 ADDRESSES										
IPV6 ADDRESSES										
Filter										
Enter property name or value										
<input type="checkbox"/>	Name	IP address	Access type	Region	Type	Version	In use by	Subnetwork	VPC Network	Network Tier
<input type="checkbox"/>	-	10.128.0.2	Internal	us-central1	Ephemeral	IPv4	VM instance servidorweb (Zone us-central1-a)	default	default	
<input type="checkbox"/>	-	10.128.0.3	Internal	us-central1	Ephemeral	IPv4	VM instance maquina-salto (Zone us-central1-a)	default	default	
<input type="checkbox"/>	-	34.66.101.236	External	us-central1	Ephemeral	IPv4	VM instance maquina-salto (Zone us-central1-a)	default	default	
<input type="checkbox"/>	-	35.193.79.220	External	us-central1	Ephemeral	IPv4	VM instance servidorweb (Zone us-central1-a)	default	default	

Se cierra la entrada de todo el tráfico no deseado a las dos máquinas, en el caso de la máquina de servidor, únicamente se le deja abierto de tráfico web y para la conexión ssh. En el caso de la máquina de salto, simplemente basta con permitir el tráfico al puerto 22.

<input type="checkbox"/>	servidor-web-externo	Ingress	web	IP ranges: 0.0.	tcp:80, 443	Allow	1000	default	Off
<input type="checkbox"/>	servidor-web-interno	Ingress	web	IP ranges: 10.	tcp:22 udp:22	Allow	1000	default	Off

Se realiza el intercambio de claves entre la máquina en la nube y la máquina personal, de forma que se pueda establecer una consola de comandos entre ambas

```
raul@Maquina1:~/.ssh$ ssh 34.66.101.236
The authenticity of host '34.66.101.236 (34.66.101.236)' can't be established.
ED25519 key fingerprint is SHA256:3Z+GULYJZZVAwfHpaQHpEk5zGf7yzwxpgCEv8XLT4Aw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '34.66.101.236' (ED25519) to the list of known hosts

linux maquina-salto 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
```

Para conectarse con el servidor web se establece la conexión ssh con la máquina de salto

```
raul@maquina-salto:~/.ssh$ 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.
```



Se le quita la dirección ip pública al servidor web para que solo pueda recibir tráfico de dentro de la red en la que se encuentra


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](#)

IP stack type

☒ IPv4 (single-stack)
☐ IPv4 and IPv6 (dual-stack)



Internal IP address

10.128.0.2

Primary internal IP
Ephemeral  

Alias IP ranges

[+ ADD IP RANGE](#)

External IPv4 address
None  

[DONE](#)

Hay que meter un Nat para poder salir todos a internet y se pueda instalar nginx en la máquina de servidor web.

Cloud NAT lets your VM instances and container pods communicate with the internet using a shared, public IP address.

Cloud NAT uses Cloud NAT gateway to manage those connections. Cloud NAT gateway is region and VPC network specific. If you have VM instances in multiple regions, you'll need to create a Cloud NAT gateway for each region. [Learn more](#)

Gateway name *
gateway-salida ?
Lowercase letters, numbers, hyphens allowed

Select Cloud Router ?

Network *
default ▼

Region *
us-central1 (Iowa) ▼ ?
One subnet.

Cloud Router *
router-salida ▼ ?

Cloud NAT mapping ?

Source (internal)
Primary and secondary ranges for all subnets ▼ ?
Select which subnets to map to the Cloud NAT gateway. Primary IP addresses are used by VM instances and secondary IP addresses are used by container pods. [Learn more](#)

Cloud NAT IP addresses
Automatic (recommended) ▼ ?

Destination (external)

Internet

✓ ADVANCED CONFIGURATIONS

CREATE CANCEL

Una vez que se ha creado el router, es posible instalar nginx

```
raul@servidorweb:~$ sudo apt install nginx
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nginx is already the newest version (1.18.0-6.1+deb11u2).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Una vez se ha creado un router que permite salir a internet, a la máquina del servidor, es necesario crear una máquina intermedia que realice el balanceo del tráfico recibido.

Para la creación de este balanceador de carga hay que crear los siguientes elementos:

- Servicio backend
- Network endpoint group
- Certificado (puesto que se recibe tráfico https)

Name *
servicio-backend
Lowercase, no spaces.

Description

Backend type
Zonal network endpoint group

Protocol
HTTP

Named port
http

Timeout *
30 seconds

Backends

Regions

us-central1

i Because you selected the standard network tier, all backends will be in one region. To use multiple regions, change your network service tier to premium in Frontend configuration. [Learn more](#)

New backend

Network endpoint group *
network-endpoint-group

Balancing mode

Rate

Maximum RPS *
10 RPS

Scope
per endpoint

CREATE

CANCEL

▼ 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

Classic HTTP(S) load balancing supports both the Premium and Standard Network Service tiers. IPv6 addresses require Premium tier. Standard tier addresses require selecting a region for the frontend. [More information](#)

- ☐ Premium (Current project-level tier, [change](#))
- ☒ Standard

IP version
IPv4 ▼

IP address
ipestatica ▼

Port
443 ▼

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

Certificate *
certificado ▼ ?

▼ ADDITIONAL CERTIFICATES

SSL policy *
GCP default ▼

QUIC negotiation
Automatic (default) ▼

- ☒ **Enable HTTP to HTTPS redirect**
Requires a reserved external IP address. Enabling HTTP to HTTPS redirect automatically generates a separate URL map with the HTTP to HTTPS redirection configuration.

Name *
serviciobackend ?

Lowercase, no spaces.

Description

Backend type
Zonal network endpoint group ▼

Protocol
HTTP ▼ ?

Named port
http ?

Timeout *
30 seconds ?

Backends

Regions

us-central1



Because you selected the standard network tier, all backends will be in one region. To use multiple regions, change your network service tier to premium in Frontend configuration. [Learn more](#)

New backend



Network endpoint group *
network-endpoint-group2 ▼

Balancing mode ?


Rate

Maximum RPS *
10 RPS

Scope
per endpoint ▼



Se puede comprobar que efectivamente funciona

balanceador


 Faster web performance and improved web protection with Cloud CDN and Cloud Armor. [Learn more](#)

[DETAILS](#) [MONITORING](#) [CACHING](#)

Frontend

Protocol 	IP:Port	Certificate	SSL Policy	Network Tier 
HTTPS	35.208.40.214:443	certificado	GCP default	Standard

Host and path rules

Hosts 	Paths	Backend
All unmatched (default)	All unmatched (default)	backendservice



Backend

Backend services




1. backendservice

Endpoint protocol	Timeout	Health check	Cloud CDN	Logging
HTTP	30 seconds	healthcheck	Disabled	Disabled

[ADVANCED CONFIGURATIONS](#)

Name 	Type	Scope	Healthy	Autoscaling	Balancing mode	Capacity
network-endpoint-group2	Zonal network endpoint group	us-central1-a	 2 of 2	No configuration	Max RPS: 10 (per endpoint)	100%

Se puede comprobar que el https offloading se ha configurado correctamente porque se han creado dos balanceadores de carga de forma simultánea, uno para la redirección del tráfico dirigido al puerto 80 y otro para el tráfico https

<input type="checkbox"/>	Name	Load balancer type 	Protocols	Region	Backends
<input type="checkbox"/>	balanceador	HTTP(S) (Classic)	HTTPS	us-central1	 1 backend service (0 instance groups, 1 network endpoint group)
<input type="checkbox"/>	balanceador-redirect	HTTP(S) (Classic)	HTTP	us-central1	

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

La principal ventaja que tiene realizar https offloading es que se fuerza a que todo el tráfico que llega al servidor, sea tráfico cifrado, es decir que cualquier persona que intente interceptar los mensajes y leer su contenido no lo va a entender.

La desventaja de implementar https offloading es que el tráfico se incrementa de forma sustancial, puesto que todas las solicitudes que no tengan como destino el puerto 443 de la máquina, o que no se traten de tráfico https se van a ver redirigidas, y por lo tanto hay tráfico innecesario llegando de forma repetida al servidor

Para la creación del certificado se va a simular que el ordenador empleado para generarlo es la propia agencia de certificación, se forma que se pueda generar el certificado de forma gratuita

[illegible]

```
cert.pem Documents KEY.key password.txt Public startup-script.sh Videos
Desktop Downloads Music Pictures snap Templates
```

Se genera un certificado el cual contiene la clave privada y un fichero con la clave pública. Ambos ficheros son cargados en la nube de Google de forma que son ellos los que lo gestionan

En el último apartado de la práctica se van a implementar políticas de seguridad en el firewall. La primera de las políticas bloquea el tráfico que no proviene de determinados países. Para este ejemplo se ha reducido la lista a cinco países miembros de la unión europea, aunque la lista se puede ampliar.

☒ Advanced mode ?

Match ?

Press Ctrl + Space to get suggestions in the editor

```
Press Alt+F1 for Accessibility Options.
1  origin.region_code == 'FR' || origin.region_code ==
   'GB' || origin.region_code == 'DE' || origin.region_code
   == 'PT' || origin.region_code == 'NL'
2
```

<input checked="" type="checkbox"/>	Allow	origin.region_code == 'FR' origin.region_code == 'GB' origin.region_code == 'DE' origin.region_code == 'PT' origin.region_code == 'NL'	2	⋮
<input type="checkbox"/>	Deny (403)	IP addresses/ranges * (All IP addresses)	Default rule, higher priority overrides it	2,147,483,647 ⋮

En un segundo apartado se protege el sistema frente a ataques de sql injection

```
1  evaluatePreconfiguredExpr('sqli-stable', [
2    'owasp-crs-v030001-id942200-sqli'
3  ])
4
```

Por último, se protege frente a ataque de cross-site scripting

Match ?

Press Ctrl + Space to get suggestions in the editor

```
Press Alt+F1 for Accessibility Options.
1  evaluatePreconfiguredExpr('xss-v33-stable',
   ['owasp-crs-v030301-id941330-xss',
    'owasp-crs-v030301-id941340-xss'])
```

block-sql	Backend security policy	2	0
block-xss	Backend security policy	2	0
seguridad	Backend security policy	3	0

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

Una opción para mejorar la disponibilidad del servidor web sería crear las máquinas virtuales en diferentes emplazamientos, de forma que, si se cae algún cpd de Google, el resto sigan disponibles.

Otra forma de aumentar la seguridad es aplicar más políticas de seguridad como por ejemplo protegerse a ataques RCE.