Práctica 1

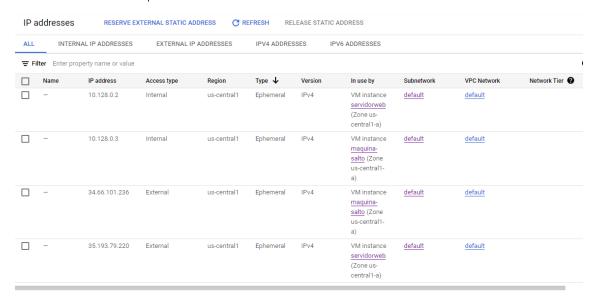
ARQUITECTURA DE SERVICIOS EN RED

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



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.



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

```
The authenticity of host '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 varning: Permanently added '34.66.101.236' (ED25519) to the list of known hosts inux 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

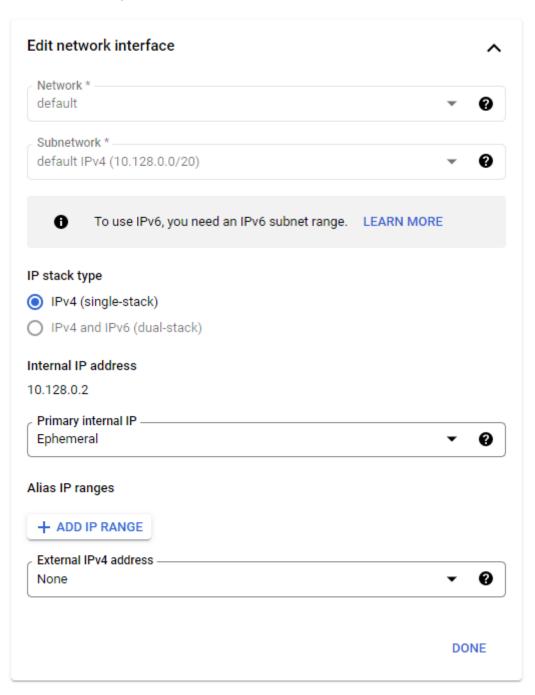
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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 @

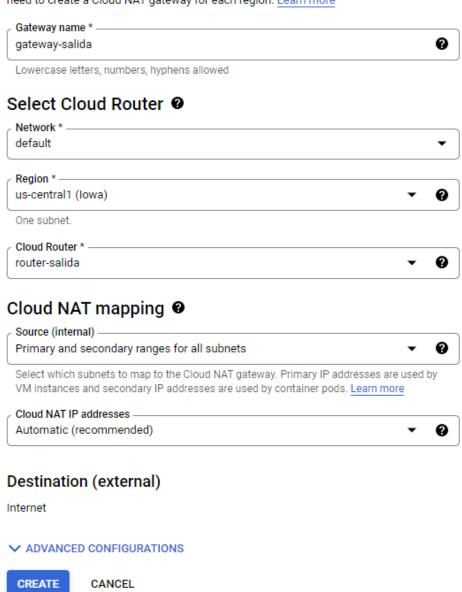
Network interface is permanent



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



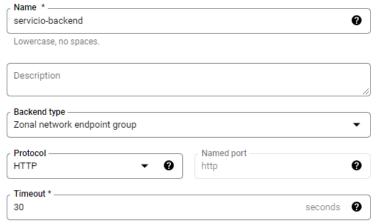
Una vez que se ha creado el router, es posible instalar nginx

```
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)

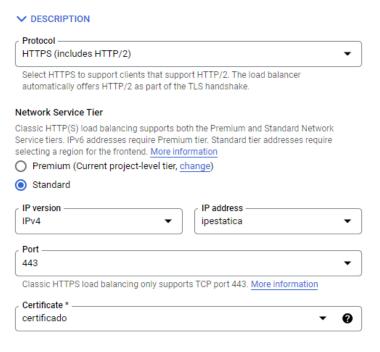


Backends Regions us-central1 Because you selected the standard network tier, all backends will be in one region. To use multiple regions, change your network service tier to premium in Frontend configuration. Learn more New backend Network endpoint group * network-endpoint-group Balancing mode ? Rate Maximum RPS * Scope

per endpoint

CREATE

CANCEL

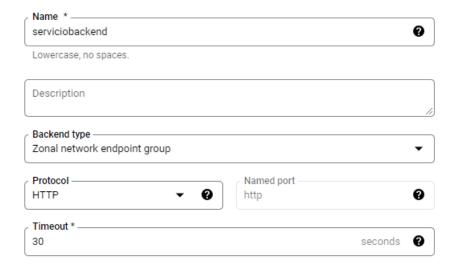


✓ ADDITIONAL CERTIFICATES



▼ 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.

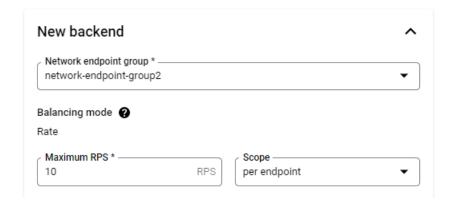


Backends

Regions

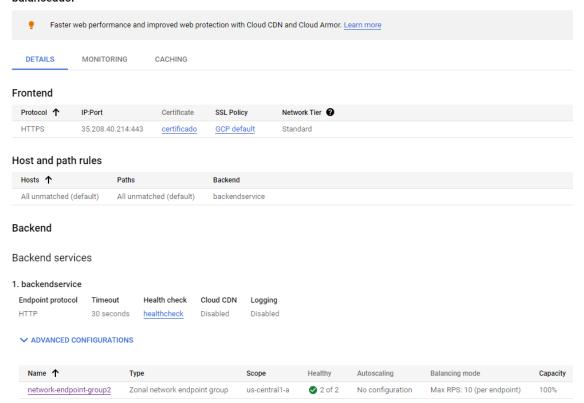
us-central1

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



Se puede comprobar que efectivamente funciona

balanceador



Se puede comprobar que el https ofloading 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



¿Qué ventajas e incovenientes 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.

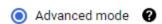
La desventaja de implementar https offloading es que el tráfico se incrementa de forma sustancial, puesto que todas las solicitudes que no tengan como destino el puerto 443 de la máquina, o que no se traten de tráfico https se van a ver redirigidas, y por lo tanto hay tráfico innecesario llegando de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

```
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.



Match @

Press Ctrl + Space to get suggestions in the editor



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.