

Nginx Proxy Inverso + Securización en Apache2

Trabajo realizado por: [David López Saorín](#)






Descripción

En esta práctica estaré usando un Nginx realizando la tarea de proxy inverso y por detrás habrán dos máquinas corriendo Apache2 por detrás: “Backend1” sirviendo una página web pública la cual podrá acceder cualquiera conociendo su dirección y “Backend2” que estará accesible siempre y cuando aporten el usuario y contraseña adecuados.

En resumen, depende la url que pidas desde el cliente, te redirigirá a la web pública o a la privada con acceso restringido.

Configuración previa

 lxc	150 (SADPI)	12.2 %	9.1 %	0.0% of 1 ...	00:02:26	0.0% of 16...	0.3 %
 lxc	151 (Back1)	13.1 %	10.0 %	20.3% of 1 ...	00:02:24	1.3% of 16...	0.3 %
 lxc	152 (Back2)	13.1 %	10.2 %	0.0% of 1 ...	00:02:22	0.0% of 16...	0.3 %

Estas son las 3 máquinas que estaré utilizando para montar la estructura. Las cuales tienen el detalle de que su Id es el último octeto de sus respectivas IPs para mayor comodidad a la hora de configurarlas.

Proxy Inverso Nginx

```
root@SADPI:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if117: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 4e:e8:59:f4:05:41 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.1.150/24 brd 172.16.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::4ce8:59ff:fef4:541/64 scope link
        valid_lft forever preferred_lft forever
root@SADPI:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04 LTS
Release:        22.04
Codename:       jammy
```

Esta es la IP que he elegido para el PI “172.16.1.150”, y su distribución es un ubuntu 22.

Apache2(Back1)

```
root@Back1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if121: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether a6:d5:de:94:ec:a5 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.1.151/24 brd 172.16.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a4d5:deff:fe94:eca5/64 scope link
        valid_lft forever preferred_lft forever
root@Back1:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04 LTS
Release:        22.04
Codename:       jammy
```

La máquina Backend1 tiene como IP la “172.16.1.151” y su distribución es también ubuntu 22.

Apache2(Back2)

```
root@Back2:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if125: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether b2:fd:01:fd:46:62 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.1.152/24 brd 172.16.1.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::b0fd:1ff:fe46:4662/64 scope link
        valid_lft forever preferred_lft forever
root@Back2:~# lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 22.04 LTS
Release:        22.04
Codename:       jammy
```

La máquina Backend2 tiene como IP la “172.16.1.152” y su distribución es de nuevo ubuntu 22.

Instalando apache2 en los Backends

```
root@Back1:/var/www/html# apt update && apt install apache2 -y
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 229 kB in 1s (226 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
139 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.52-1ubuntu4.7).
0 upgraded, 0 newly installed, 0 to remove and 139 not upgraded.
```

```
root@Back2:~# apt update && apt install apache2 -y
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 229 kB in 1s (238 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
139 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
apache2 is already the newest version (2.4.52-1ubuntu4.7).
```

El primer paso será instalar Apache2 en ambas máquinas backend con el comando “apt update && apt install apache2 -y”.

Index de default Back1 (Página web pública)

```
root@Back1:~# cat /var/www/html/index.html
<!DOCTYPE html>
<html>
  <head>
    <title>Web publica <!-- Replace 'X' with '1' or '2' as appropriate --></title>
```

En backend1 utilizaré la configuración por defecto de Apache2 para servir la página web pública, pero yo cambio el index.html y le introduzco el código que se puede ver en la imagen.

Configuración de Back2 (Página web privada)

```
root@Back2:/etc/apache2/sites-available# cat 000-default.conf | grep -v "#"
<VirtualHost *:80>

    ServerAdmin admin@privada.com
    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory /var/www/html>
        Options Indexes
        AuthType Basic
        AuthName "ACCESO RESTRINGIDO A LA INTRANET"
        AuthBasicProvider file
        AuthUserFile "/opt/apache2/privada.com/passwords"
        Require valid-user
    </Directory>
</VirtualHost>
```

Este es el archivo por defecto que se encuentra en sites-available, el cual yo cambio con los parámetros que se aprecian, añadiendo a éste la obligación de pedir usuario y contraseña al cliente que quiera conectarse.

El archivo de donde sacará la contraseña y usuario con permisos está en “/opt/apache2/privada.com/passwords”

```
root@Back2:/etc/apache2/sites-available# cat /var/www/html/index.html
<!DOCTYPE html>
<html>
  <head>
    <title>Web Privada <!-- Replace 'X' with '1' or '2' as appropriate --></title>
```

Aquí se puede apreciar como el código del index lo modifíco para que salga de título “Web Privada y diferenciarlo del otro sitio”

```
root@Back2:~# mkdir -p /opt/apache2/privada.com
root@Back2:~# sudo htpasswd -c /opt/apache2/privada.com/passwords david
New password:
Re-type new password:
Adding password for user david
```

A continuación, creo la ruta antes mencionada donde se almacenará el usuario y contraseña, y con el comando “sudo htpasswd -c /opt/apache2/privada.com/passwords david” le indico el archivo donde se guardará y el usuario con los permisos. Después hay que introducir la contraseña de ese usuario web.

Configuración de Nginx Proxy Inverso

```
root@SADPI:/etc/nginx/conf.d# apt update && apt install nginx -y
Hit:1 http://archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Fetched 229 kB in 1s (236 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
140 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nginx is already the newest version (1.18.0-6ubuntu14.4).
0 upgraded, 0 newly installed, 0 to remove and 140 not upgraded.
```

Primero hay que instalar Nginx en el LXC para comenzar con la configuración.

```
root@SADPI:/etc/nginx/conf.d# cat revproxy.conf
server{
    listen 80;
    server_name publica.com;

    location / {
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_pass http://172.16.1.151/;
    }
}
server{
    listen 80;
    server_name privada.com;

    location / {
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $remote_addr;
        proxy_pass http://172.16.1.152/;
    }
}
```

Y este es el archivo final de la configuración del proxy inverso, el cual le indico los dos servidores que estarán escuchando por el puerto 80, uno será “publica.com” y el otro “privada.com”, con sus respectivas IPs y el reenvío de cabeceras de las IPs de los clientes.

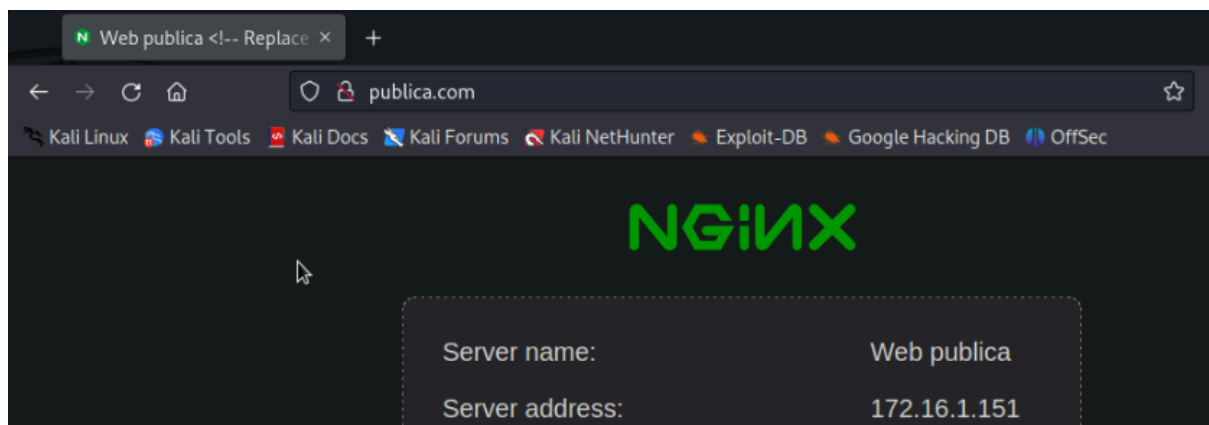
Configuración en el cliente

```
(kali㉿kali)-[~]  
$ cat /etc/hosts  
127.0.0.1    localhost  
127.0.1.1    kali  
#172.16.1.10  balanceo.com palo.com  
#172.16.1.103 storedavid.com appdavid.com  
#192.168.4.11 ed2phpserver.com  
172.16.1.150 publica.com privada.com  
# The following lines are desirable for IPv6 capable hosts  
::1          localhost ip6-localhost ip6-loopback  
ff02::1     ip6-allnodes  
ff02::2     ip6-allrouters
```

Para que el cliente pueda ver las direcciones antes configuradas hay que introducir la IP apuntando al servidor Nginx con los nombres de dominio a los redirigir.

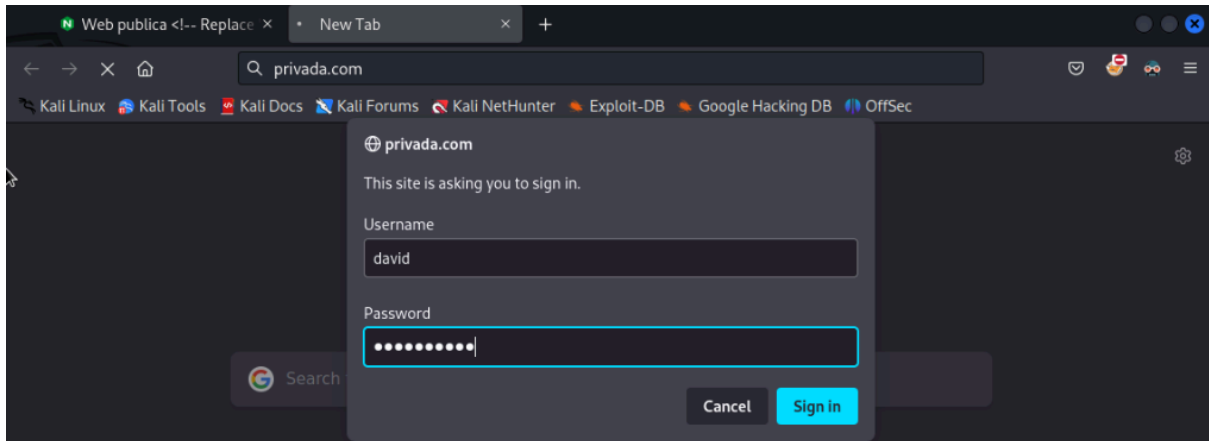
Verificación del funcionamiento

Web Pública

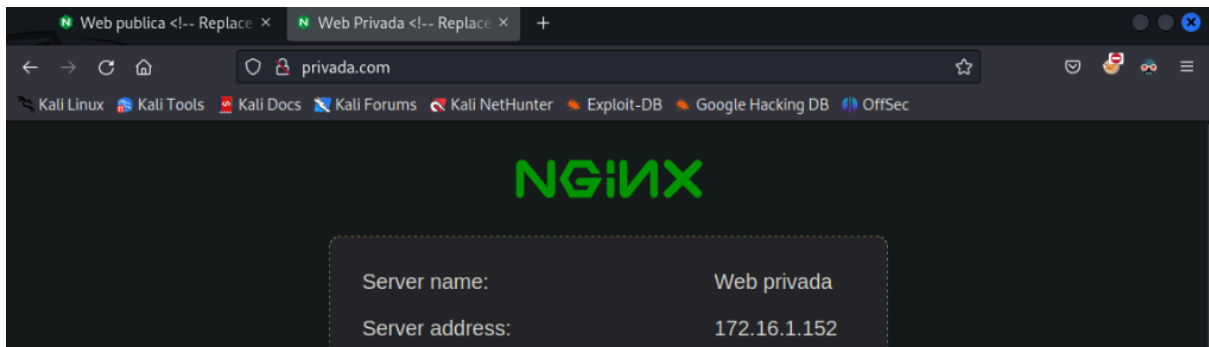


Entro a la web pública desde el navegador y funciona :).

Web Privada



Cuando intento entrar a la web privada me pide introducir las credenciales correspondientes y...



Consigo entrar... Funciona!!