

## REENVIOS DE PUERTOS : DESDE LA RED INTERNA A LA RED INTERNA

En esta parte vamos a realizar una configuración de iptables para que podamos ver nuestro servidor web hospedado en un máquina virtual dentro de la red interna (192.168.1.3).

Voy a explicarte cómo hacerlo paso a paso:

Nosotros teníamos un montón de reglas que no servían, todo esto como resultado de los intentos fallidos. Decidimos borrar todas las reglas de iptables, también se nos eliminara la que nos permite la salida de la red interna a la externa, pero después la volveremos a configurar.

***Ejecutamos los siguientes comandos para eliminar todas las reglas actuales:***

```
iptables -F
iptables -t nat -F
iptables -t mangle -F
```

***Establece las políticas por defecto para aceptar el tráfico.***

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

## Paso 2: Configurar la Redirección de Puertos

Para redirigir el tráfico de la IP pública (100.77.20.21) en los puertos 80 y 443 hacia el servidor Nginx en la IP interna (192.168.1.3), usamos las siguientes reglas de iptables:

Redirige el tráfico entrante en el puerto 80 (HTTP) al servidor Nginx en la IP interna

```
iptables -t nat -A PREROUTING -p tcp -d 100.77.20.21 --dport 80 -j
DNAT --to-destination 192.168.1.3:80
```

Del mismo modo redirigimos el tráfico entrante en el puerto 443 (HTTPS) al servidor Nginx en la IP interna

```
iptables -t nat -A PREROUTING -p tcp -d 100.77.20.21 --dport 443 -j
DNAT --to-destination 192.168.1.3:443
```

### Paso 3: Configurar el Enmascaramiento (Masquerading) para Salida a Internet

Para que las máquinas en la red interna (192.168.1.0/24) puedan acceder a Internet usando la IP pública de tu router (100.77.20.21), agrega la siguiente regla en la cadena

#### POSTROUTING:

```
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o *interfaz* -j MASQUERADE
```

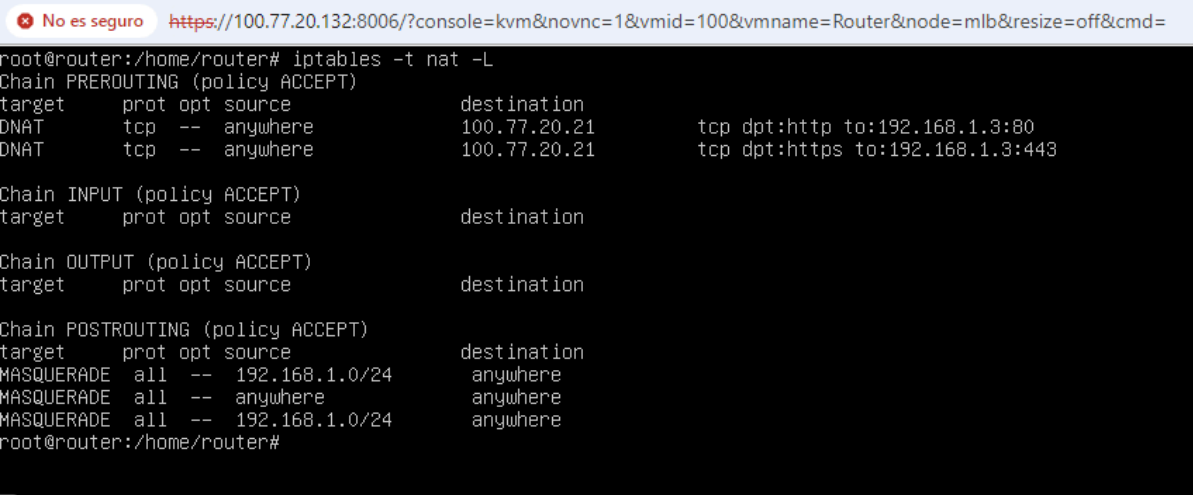
**Nota:** Reemplaza *\*interfaz\** con el nombre de la interfaz de red que está conectada a Internet en tu router virtual. ( ens18 en nuestro caso )

### Paso 4: Guardar las Reglas de iptables

Una vez que hayas configurado las reglas, guarda la configuración para que se mantenga después de reiniciar:

Únicamente guardamos las reglas para que no se borren

```
iptables-save > /etc/iptables/rules.v4
```



```
root@router:/home/router# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination
DNAT       tcp  --  anywhere               100.77.20.21           tcp dpt:http to:192.168.1.3:80
DNAT       tcp  --  anywhere               100.77.20.21           tcp dpt:https to:192.168.1.3:443

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  --  192.168.1.0/24        anywhere
MASQUERADE all  --  anywhere              anywhere
MASQUERADE all  --  192.168.1.0/24        anywhere
root@router:/home/router#
```

## INSTALACIÓN DE PHP

```
root@nginx:/home/nginx# apt search php-fpm
Ordenando... Hecho
Buscar en todo el texto... Hecho
php-cgi/jammy 2:8.1+92ubuntu1 all
  server-side, HTML-embedded scripting language (CGI binary) (default)

php-fpm/jammy 2:8.1+92ubuntu1 all
  server-side, HTML-embedded scripting language (FPM-CGI binary) (default)

php-symfony-runtime/jammy 5.4.4+dfsg-1ubuntu8 all
  decouple PHP applications from global state
```

```
root@nginx:/home/nginx# apt install php-fpm
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
php-fpm ya está en su versión más reciente (2:8.1+92ubuntu1).
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 4 no actualizados.
root@nginx:/home/nginx# apt install php-fpm
```

## ROUTER

No es seguro <https://100.77.20.132:8006/?console=kvm&novnc=1&vmid=100&vmname=Router&node=mlb&resize=off&cmd=>

```
root@router:/home/router# iptables -P INPUT ACCEPT
root@router:/home/router# iptables -P FORWARD ACCEPT
root@router:/home/router# iptables -P OUTPUT ACCEPT
root@router:/home/router# iptables -t nat -A PREROUTING -p tcp -d 100.77.20.21 --dport 80 -j DNAT --to-destination 192.168.1.3:80
root@router:/home/router# iptables -t nat -A PREROUTING -p tcp -d 100.77.20.21 --dport 443 -j DNAT --to-destination 192.168.1.3:443
root@router:/home/router#
```

```
root@router:/home/router# iptables -P INPUT ACCEPT
root@router:/home/router# iptables -P FORWARD ACCEPT
root@router:/home/router# iptables -P OUTPUT ACCEPT
root@router:/home/router# iptables -t nat -A PREROUTING -p tcp -d 100.77.20.21 --dport 80 -j DNAT --to-destination 192.168.1.3:80
root@router:/home/router# iptables -t nat -A PREROUTING -p tcp -d 100.77.20.21 --dport 443 -j DNAT --to-destination 192.168.1.3:443
root@router:/home/router# #iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o
root@router:/home/router# ipa
Command 'ipa' not found, but can be installed with:
apt install freeipa-client
root@router:/home/router# 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: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:d8:ee:ae brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 100.77.20.21/24 metric 100 brd 100.77.20.255 scope global dynamic ens18
        valid_lft 28253sec preferred_lft 28253sec
    inet6 fe80::be24:11ff:fed8:eeae/64 scope link
        valid_lft forever preferred_lft forever
3: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:b6:f4:97 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.1.1/24 brd 192.168.1.255 scope global ens19
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:feb6:f497/64 scope link
        valid_lft forever preferred_lft forever
root@router:/home/router# iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o ens19 -j MASQUERADE
root@router:/home/router#
```

## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*