

Permitiendo que solo pueda escuchar por la ip privada con puerto 8080

```
sebastian.gonzalezvarela@vm-131-214: ~  
GNU nano 4.8 /etc/nginx/sites-enabled/default  
server {  
    listen 172.24.131.214:8080 default_server;  
    listen 8080 default_server;  
    listen [::]:8080 default_server;  
    listen 80 default_server;  
    listen [::]:80 default_server;  
}
```

Viendo que se puede conectar por la IP privada del servidor principal desde el router

```
sung.moon@vm-131-223:~$ curl --connect-timeout 5 172.24.131.214  
<!DOCTYPE html>  
<html>  
<head>  
<title>Welcome to nginx!</title>  
<style>  
    body {  
        width: 35em;  
        margin: 0 auto;  
        font-family: Tahoma, Verdana, Arial, sans-serif;  
    }  
</style>  
</head>  
<body>  
<h1>Welcome to nginx!</h1>  
<p>If you see this page, the nginx web server is successfully installed and  
working. Further configuration is required.</p>  
  
<p>For online documentation and support please refer to  
<a href="http://nginx.org/">nginx.org</a>.<br/>  
Commercial support is available at
```

```
# Note: This may impact IPv6 TCP sessions too  
#net.ipv4.tcp_syncookies=1  
  
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1  
  
# Uncomment the next line to enable packet forwarding for IPv6  
# Enabling this option disables Stateless Address Autoconfiguration  
# based on Router Advertisements for this host
```

```
sung.moon@vm-131-223: ~
GNU nano 4.8 /etc/iptables/rules.v4
# Generated by iptables-save v1.8.4 on Mon Jul 26 14:24:15 2021
*filter
:INPUT ACCEPT [344895:411185288]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [57714:9348186]
:vcl-inuse - [0:0]
:vcl-post_load - [0:0]
-A INPUT -m comment --comment "VCL: jump to rules added during the inuse stage of reservation 63766 (2021-07-12 17:03:00)" -j vcl-inuse
-A INPUT -m comment --comment "VCL: jump to rules added during the post-load stage (2021-05-07 01:36:53)" -j vcl-post_load
-A vcl-inuse -s 172.17.0.15/32 -p tcp -m comment --comment "VCL: allow traffic from 172.17.0.15 to tcp/3389 during the inuse stage" -j ACCEPT
-A vcl-inuse -s 172.17.0.15/32 -p tcp -m comment --comment "VCL: allow traffic from 172.17.0.15 to tcp/22 during the inuse stage" -j ACCEPT
-A vcl-inuse -s 172.17.4.5/32 -p tcp -m comment --comment "VCL: allow traffic from 172.17.4.5 to tcp/3389 during the inuse stage" -j ACCEPT
-A vcl-inuse -s 172.17.4.5/32 -p tcp -m comment --comment "VCL: allow traffic from 172.17.4.5 to tcp/22 during the inuse stage" -j ACCEPT
-A vcl-post_load -s 172.24.127.105/32 -m comment --comment "VCL: allow traffic from management node (2021-05-07 01:36:53)" -j ACCEPT
COMMIT
# Completed on Mon Jul 26 14:24:15 2021

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text   ^J Justify    ^C Cur_Pos   M-L Undo     M-A Mark Text
^X Exit      ^R Read File  ^T Replace   ^L Paste Text ^I To Spell   ^G Go To Line M-E Redo     M-B Copy Text
```

```
Last login: Mon Jul 26 14:32:51 2021 from 172.17.0.3
sung.moon@vm-131-223:~$ sudo iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT ACCEPT
-N ICMP
-N TCP
-N UDP
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -p udp -m conntrack --ctstate NEW -j UDP
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j TCP
-A INPUT -p icmp -m conntrack --ctstate NEW -j ICMP
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -j REJECT --reject-with icmp-proto-unreachable
-A TCP -p tcp -m tcp --dport 22 -j ACCEPT
sung.moon@vm-131-223:~$
```

Prerouting and post routing

```
sung.moon@vm-131-223:~$ sudo iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 8080 -j DNAT --to-destination 172.24.131.214
sung.moon@vm-131-223:~$ sudo iptables -t nat -A POSTROUTING -o eth1 -p tcp --dport 80 -d 172.24.131.214 -j SNAT --to-source 172.24.131.223
sung.moon@vm-131-223:~$
```

```
sun@moon:~$ sudo iptables -F
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT ACCEPT
-N ICMP
-N TCP
-N UDP
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m conntrack --ctstate INVALID -j DROP
-A INPUT -p udp -m conntrack --ctstate NEW -j UDP
-A INPUT -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j TCP
-A INPUT -p icmp -m conntrack --ctstate NEW -j ICMP
-A INPUT -p udp -j REJECT --reject-with icmp-port-unreachable
-A INPUT -p tcp -j REJECT --reject-with tcp-reset
-A INPUT -j REJECT --reject-with icmp-proto-unreachable
-A FORWARD -i eth0 -o eth1 -p tcp -m tcp --dport 80 --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -i eth0 -o eth1 -p tcp -m tcp --dport 80 --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -i eth0 -o eth1 -p tcp -m tcp --dport 8080 --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -i eth0 -o eth1 -p tcp -m tcp --dport 80 --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j ACCEPT
-A FORWARD -i eth0 -o eth1 -p tcp -m tcp --dport 8080 --tcp-flags FIN,SYN,RST,ACK SYN -m conntrack --ctstate NEW -j ACCEPT
-A TCP -p tcp -m tcp --dport 22 -j ACCEPT
sung.moon@vm-131-223:~$
```