

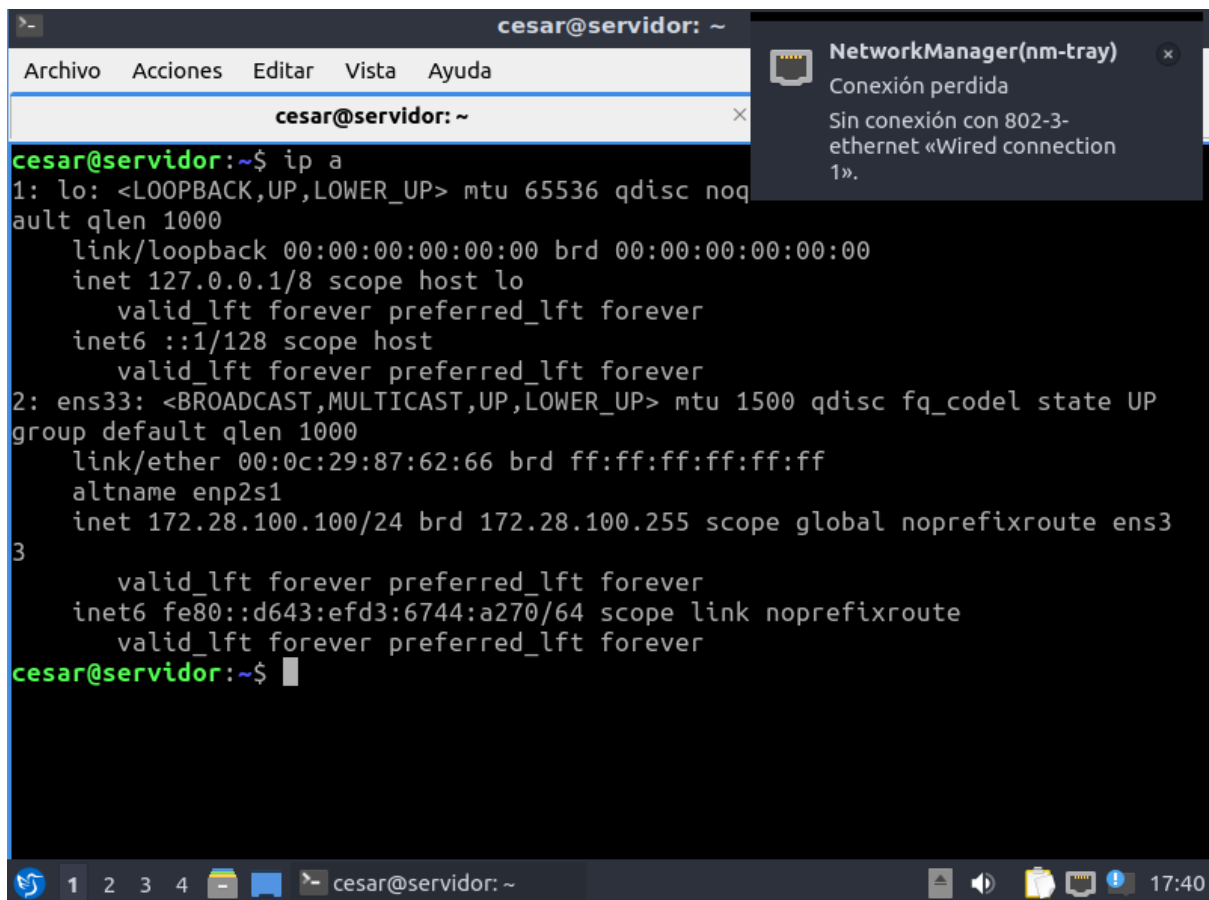
# Dnat con Iptables

## Ips e interfaces de cada maquina:

Para hacer esta práctica he puesto el cliente en una red distinta a la del equipo con los servicios ssh y nginx para simular una red externa publica que no tendría acceso normalmente a la red interna.

### **Maquina servidor:**

Esta en la vmnet2 con ip 172.28.100.100



```
cesar@servidor: ~  
Archivo Acciones Editar Vista Ayuda  
cesar@servidor: ~  
cesar@servidor:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue  
    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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP  
   group default qlen 1000  
    link/ether 00:0c:29:87:62:66 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 172.28.100.100/24 brd 172.28.100.255 scope global noprefixroute ens33  
        valid_lft forever preferred_lft forever  
3: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP  
   group default qlen 1000  
    link/ether 00:0c:29:87:62:66 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet6 fe80::d643:efd3:6744:a270/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
cesar@servidor:~$
```

Esta en bridge, vmnet2 y vmnet3.

```
Usage of /: 47.2% of 9.75GB  Swap usage: 0%  Users logged in: 0

42 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Nov 15 11:13:22 UTC 2022 on tty1
cesar@firewall:~$ 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: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6e:72:bb brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.34/24 brd 192.168.1.255 scope global ens3
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:72bb/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6e:72:c5 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 172.28.100.1/24 brd 172.28.100.255 scope global ens37
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:72c5/64 scope link
        valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:6e:72:cf brd ff:ff:ff:ff:ff:ff
    altname enp2s6
    inet 192.168.100.1/24 brd 192.168.100.255 scope global ens38
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe6e:72cf/64 scope link
        valid_lft forever preferred_lft forever
cesar@firewall:~$ _
```

Esta en vmnet3 con ip 192.168.100.100 y sin puerta de enlace.

```
cesar@cliente: ~  
Archivo Acciones Editar Vista Ayuda  
cesar@cliente: ~  
cesar@cliente:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP  
group default qlen 1000  
    link/ether 00:0c:29:cc:ce:8a brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.100.100/24 brd 192.168.100.255 scope global noprefixroute en  
s33  
        valid_lft forever preferred_lft forever  
    inet6 fe80::d8f1:4f3b:a8d3:4df5/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
cesar@cliente:~$ ip r  
192.168.100.0/24 dev ens33 proto kernel scope link src 192.168.100.100 metric  
100  
cesar@cliente:~$
```

# Instalación de los servicios SSH y Nginx

Instalar los servicios no tiene mas que un apt install con el correspondiente programa y listo. Si no cambiamos nada, el ssh usará el puerto 22 y el nginx el 80.

## Captura del ssh funcionando

```
cesar@servidor: ~
Archivo Acciones Editar Vista Ayuda
cesar@servidor: ~
cesar@servidor:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset:
   Active: active (running) since Wed 2022-11-16 17:31:48 CET; 15min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 789 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCE
 Main PID: 825 (sshd)
    Tasks: 1 (limit: 2189)
   Memory: 3.5M
      CPU: 16ms
   CGroup: /system.slice/ssh.service
           └─825 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

nov 16 17:31:46 servidor systemd[1]: Starting OpenBSD Secure Shell server...
nov 16 17:31:48 servidor sshd[825]: Server listening on 0.0.0.0 port 22.
nov 16 17:31:48 servidor sshd[825]: Server listening on :: port 22.
nov 16 17:31:48 servidor systemd[1]: Started OpenBSD Secure Shell server.
lines 1-17/17 (END)
```

## Captura del nginx funcionando

```
cesar@servidor: ~
cesar@servidor:~$ systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor pres
   Active: active (running) since Wed 2022-11-16 17:31:51 CET; 20min ago
     Docs: man:nginx(8)
   Process: 786 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_pro
   Process: 858 ExecStart=/usr/sbin/nginx -g daemon on; master_process on;
 Main PID: 859 (nginx)
    Tasks: 3 (limit: 2189)
   Memory: 8.9M
      CPU: 36ms
   CGroup: /system.slice/nginx.service
           └─859 "nginx: master process /usr/sbin/nginx -g daemon on; mast
             └─860 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" ""
             └─861 "nginx: worker process" "" "" "" "" "" "" "" "" "" "" ""

nov 16 17:31:46 servidor systemd[1]: Starting A high performance web server
nov 16 17:31:51 servidor systemd[1]: Started A high performance web server a
lines 1-17/17 (END)
```

## Configuración en el cortafuegos.

Lo primero es activar el forward en el archivo sysctl.conf.

```
GNU nano 6.2 /etc/sysctl.conf *
#
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.
#
#kernel.domainname = example.com
#
# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3
#
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# 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
```

Ponemos las políticas por defecto en DROP y permitimos las conexiones ssh para poder trabajar mejor desde el mobaXterm.

```
root@firewall:/home/cesar# iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
-A INPUT -i ens33 -p tcp -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o ens33 -m state --state ESTABLISHED -j ACCEPT
root@firewall:/home/cesar# _
```

Ahora vamos a declarar las normas de prerouting para que el cliente pueda conectarse al servidor. Para ello vamos a ver que puertos estan ya en uso en el firewall y asi coger uno libre.

```
cesar@firewall:~$ ss -ltnp
State      Recv-Q    Send-Q    Local Address:Port      Peer Address:Port      Process
LISTEN     0          4096      127.0.0.53:53            0.0.0.0:*                systemd
LISTEN     0          128       0.0.0.0:22               0.0.0.0:*                sshd
LISTEN     0          128       127.0.0.1:6010           0.0.0.0:*                x11vnc
LISTEN     0          128       127.0.0.1:6011           0.0.0.0:*                x11vnc
LISTEN     0          128       [::]:22                  [::]:*                   x11vnc
LISTEN     0          128       [::1]:6010               [::]:*                   x11vnc
LISTEN     0          128       [::1]:6011               [::]:*                   x11vnc
cesar@firewall:~$
```

Vemos que el puerto 80 esta libre, así que será el que asignemos para la conexión http. Por el contrario el puerto 22 ya esta en uso para la conexión ssh hacia el propio firewall, por lo que tendremos que usar otro. En este caso usaremos el 50000 que no tiene ningún uso preestablecido como pudiera ser el 443(HTTPS). He tenido que activar el forward porque si no, con todo en drop, la conexión no se realizaba.

### Activación del forward entre los dos interfaces.

```
root@firewall:/home/cesar# iptables -I FORWARD -o ens38 -s 172.28.100.100/32 -j ACCEPT
root@firewall:/home/cesar# iptables -I FORWARD -i ens38 -d 172.28.100.100/32 -j ACCEPT
root@firewall:/home/cesar#
```

Aun habiendo activado el forward se puede ver más adelante que los ping siguen sin ir, por lo que solo se esta permitiendo el tipo de conexiones que nosotros permitamos mas adelante.

### Captura del comando a introducir para permitir el ssh.

```
root@firewall:/home/cesar# iptables -t nat -I PREROUTING -i ens38 -p tcp --dport 50000 -j DNAT --to-destination 172.28.100.100:22
root@firewall:/home/cesar#
```

### Captura de que el ssh esta funcionando pero el ping no.

```
cesar@cliente:~$ ssh cesar@192.168.100.1 -p 50000
cesar@192.168.100.1's password:
Permission denied, please try again.
cesar@192.168.100.1's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

0 updates can be applied immediately.

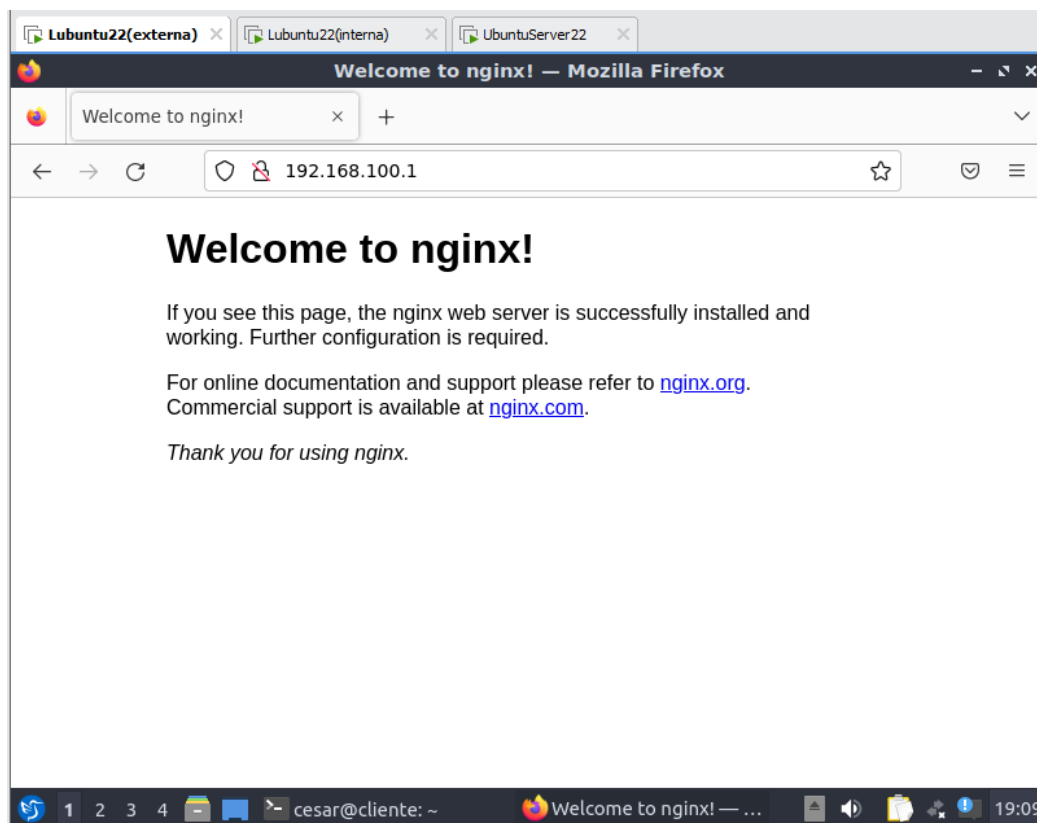
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Wed Nov 16 18:57:44 2022 from 192.168.100.100
cesar@servidor:~$ exit
logout
Connection to 192.168.100.1 closed.
cesar@cliente:~$ ping 172.28.100.100 -c 1
ping: connect: Network is unreachable
cesar@cliente:~$
```

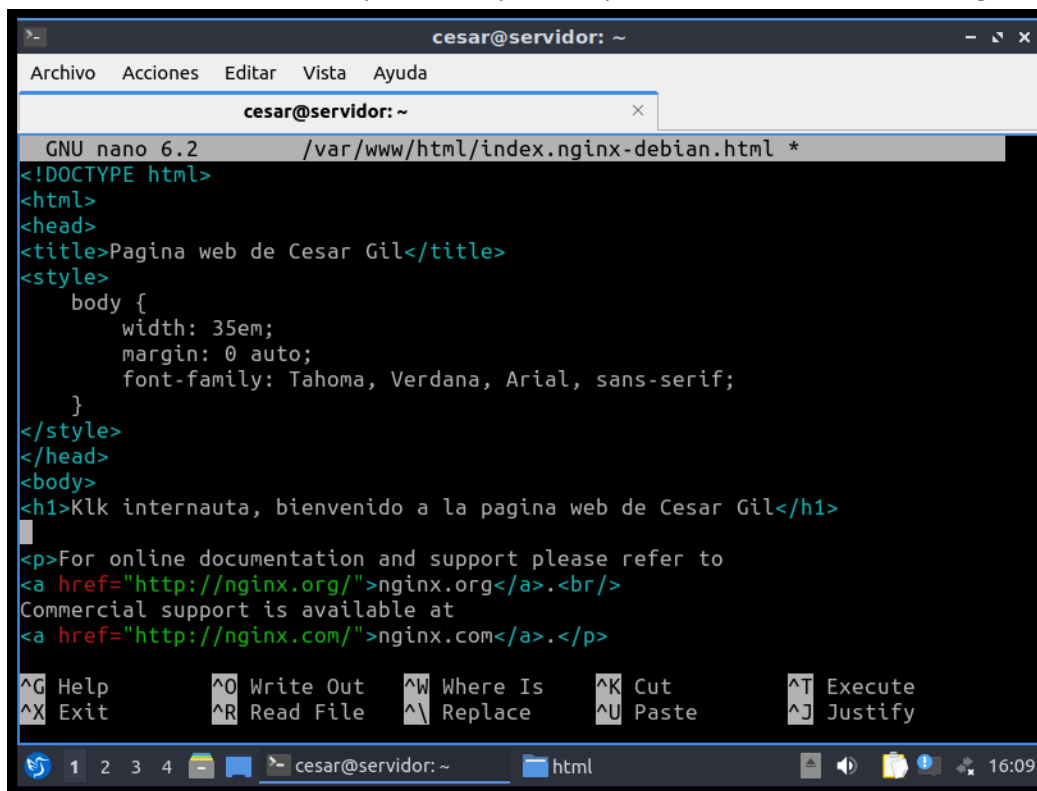
### Captura del comando a introducir para permitir el http

```
root@firewall:/home/cesar# iptables -t nat -I PREROUTING -i ens38 -p tcp --dport 80 -j DNAT --to-destination 172.28.100.100
root@firewall:/home/cesar#
```

## Captura de que la conexión http funciona



Vamos a cambiar el html para ver que se aplican los cambios al recargar la pagina.



Ahora reiniciamos el nginx y vamos a la maquina cliente a ver si se han aplicado los cambios.

```
cesar@servidor:~$ sudo systemctl restart nginx
cesar@servidor:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-11-18 16:11:55 CET; 6s ago
     Docs: man:nginx(8)
  Process: 2051 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on;
  Process: 2052 ExecStart=/usr/sbin/nginx -g daemon on; master_process on;
 Main PID: 2053 (nginx)
    Tasks: 3 (limit: 2189)
   Memory: 3.3M
      CPU: 11ms
   CGroup: /system.slice/nginx.service
           └─2053 "nginx: master process /usr/sbin/nginx -g daemon on; master_process on;"
             └─2054 "nginx: worker process"
               └─2055 "nginx: worker process"

nov 18 16:11:55 servidor systemd[1]: Starting A high performance web server: nginx.
nov 18 16:11:55 servidor systemd[1]: Started A high performance web server: nginx.
lines 1-17/17 (END)
```

### Captura de los cambios desde el cliente



### Listado de reglas iptables utilizadas.

```
root@firewall:/home/cesar# iptables -S
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
-A INPUT -i ens33 -p tcp -m tcp --dport 22 -j ACCEPT
-A FORWARD -d 172.28.100.100/32 -i ens38 -j ACCEPT
-A FORWARD -s 172.28.100.100/32 -o ens38 -j ACCEPT
-A OUTPUT -o ens33 -m state --state ESTABLISHED -j ACCEPT
root@firewall:/home/cesar# iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-A PREROUTING -i ens38 -p tcp -m tcp --dport 80 -j DNAT --to-destination 172.28.100.100
-A PREROUTING -i ens38 -p tcp -m tcp --dport 50000 -j DNAT --to-destination 172.28.100.100:22
root@firewall:/home/cesar#
```