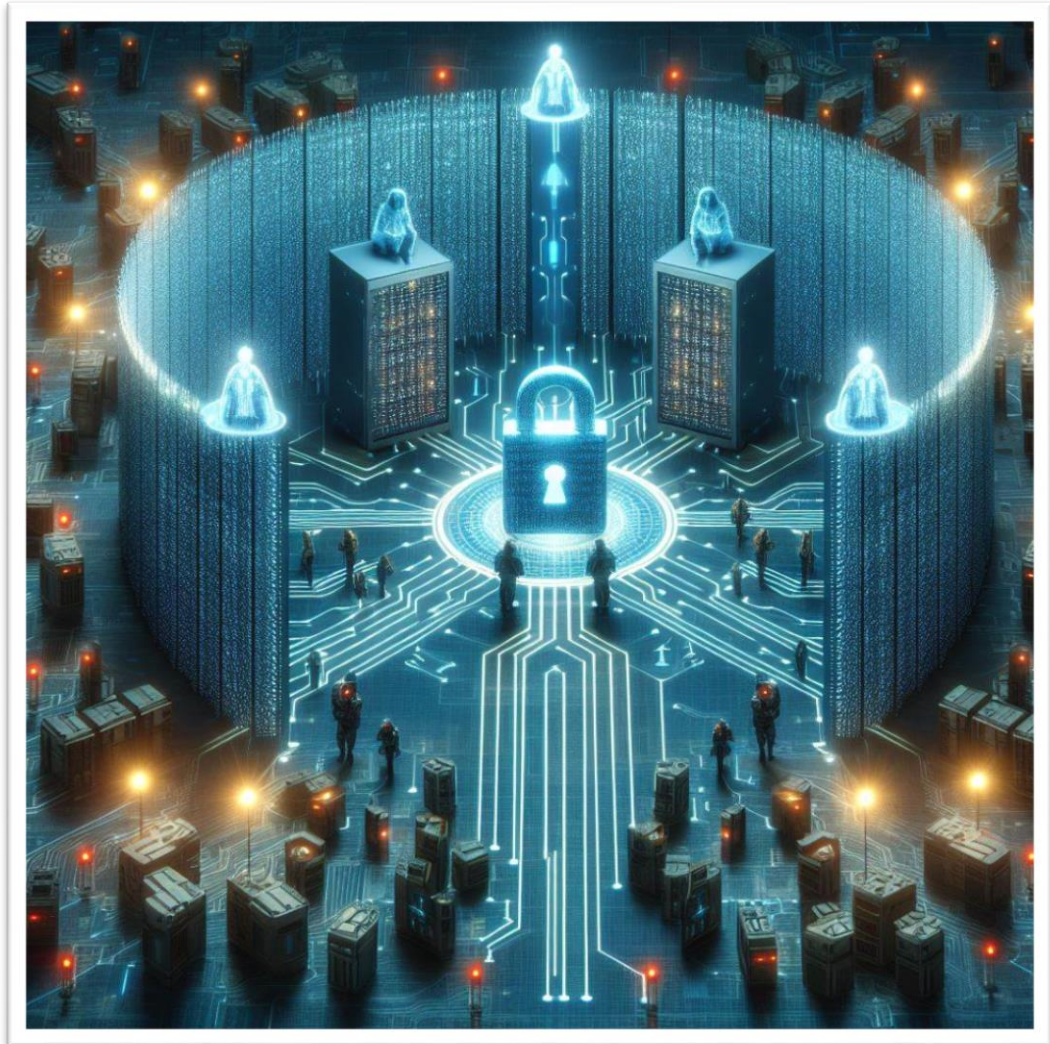


ERIC SERRANO MARÍN



ACT0502 – FIREWALLS CON NETFILTER (IPTABLES / EBTABLES)

Bastionado de Redes y Sistemas

ERIC SERRANO MARÍN

CETI

Contenido

Contenido	1
Configuración de Firewall y Servidor Web.	2
Servidor.....	2
Comprobaciones.....	3
Configuración de Firewall	4
Reglas iptables	4
Conclusiones	6

Configuración de Firewall y Servidor Web.

Configuración de red del Firewall.

Edit: Network Device (veth)

Name:	eth1	IPv4:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC address:	BC:24:11:4C:00:19	IPv4/CIDR:	192.168.0.1/24
Bridge:	vmbr100	Gateway (IPv4):	192.168.0.1
VLAN Tag:	178	IPv6:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> SLAAC
Firewall:	<input checked="" type="checkbox"/>	IPv6/CIDR:	None
		Gateway (IPv6):	

Help
Advanced ☐
OK
Reset

Configuración de red del Proxy Inverso.

Edit: Network Device (veth)

Name:	eth1	IPv4:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC address:	BC:24:11:BE:DD:21	IPv4/CIDR:	192.168.0.11/24
Bridge:	vmbr100	Gateway (IPv4):	192.168.0.1
VLAN Tag:	178	IPv6:	<input checked="" type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> SLAAC
Firewall:	<input checked="" type="checkbox"/>	IPv6/CIDR:	None
		Gateway (IPv6):	

Help
Advanced ☐
OK
Reset

Servidor

ip link set dev eth0 down

```

root@Proxy-Inverso:~# ip link set dev eth0 down
root@Proxy-Inverso:~# ip link show eth0
2: eth0@if892: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT group default qlen 1000
    link/ether bc:24:11:9c:d6:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
root@Proxy-Inverso:~#

```

Comprobaciones

Ping de Firewall a Proxy Inverso.

The left terminal shows the configuration of the Proxy Inverso interface. The right terminal shows the configuration of the Firewall interface and a successful ping from the Firewall to the Proxy Inverso.

```

root@Proxy-Inverso:~# 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@if892: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether bc:24:11:9c:d6:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
3: eth1@if896: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:9c:d6:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.0.1/24 brd 192.168.0.255 scope global eth1
        valid lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febd:d421/64 scope link
        valid lft forever preferred_lft forever
root@Proxy-Inverso:~#

root@Firewall:~# ping 192.168.0.11
PING 192.168.0.11 (192.168.0.11) 56(84) bytes of data.
64 bytes from 192.168.0.11: icmp_seq=1 ttl=64 time=0.535 ms
64 bytes from 192.168.0.11: icmp_seq=2 ttl=64 time=0.059 ms
64 bytes from 192.168.0.11: icmp_seq=3 ttl=64 time=0.059 ms
^C
--- 192.168.0.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms
rtt min/avg/max/mdev = 0.059/0.217/0.535/0.224 ms
root@Firewall:~#
  
```

Ping de Proxy Inverso a Firewall.

The left terminal shows the configuration of the Proxy Inverso interface. The right terminal shows the configuration of the Firewall interface and a successful ping from the Proxy Inverso to the Firewall.

```

root@Proxy-Inverso:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.225 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.065 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.062 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.064 ms
^C
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3071ms
rtt min/avg/max/mdev = 0.062/0.104/0.225/0.069 ms
root@Proxy-Inverso:~#

root@Firewall:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.204 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.057 ms
^C
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.057/0.094/0.204/0.063 ms
root@Firewall:~#
  
```

Ping de Firewall a PC externo.

The left terminal shows the configuration of the PC-Externo interface. The right terminal shows the configuration of the Firewall interface and a successful ping from the Firewall to the PC-Externo.

```

root@PC-Externo:~# 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@if869: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:9c:d6:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.22.229.13/16 brd 172.22.255.255 scope global dynamic eth0
        valid lft 1911sec preferred_lft 1911sec
    inet6 fe80::be24:11ff:febd:d421/64 scope link
        valid lft forever preferred_lft forever
3: eth1@if873: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether bc:24:11:9c:d6:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet6 fe80::be24:11ff:febd:d421/64 scope link
        valid lft forever preferred_lft forever
root@PC-Externo:~#

root@Firewall:~# ping 172.22.229.13
PING 172.22.229.13 (172.22.229.13) 56(84) bytes of data.
64 bytes from 172.22.229.13: icmp_seq=1 ttl=64 time=0.204 ms
64 bytes from 172.22.229.13: icmp_seq=2 ttl=64 time=0.058 ms
64 bytes from 172.22.229.13: icmp_seq=3 ttl=64 time=0.057 ms
^C
--- 172.22.229.13 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3076ms
rtt min/avg/max/mdev = 0.057/0.094/0.204/0.063 ms
root@Firewall:~#
  
```

Configuración de Firewall

Configuración de forwarding en Firewall.

```
root@Firewall:~# sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
root@Firewall:~#
```

Reglas iptables

Limpiamos las reglas iptables.

```
root@Firewall:~# iptables -F
root@Firewall:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@Firewall:~#
```

Limpiamos también las reglas de la tabla NAT.

```
root@Firewall:~# iptables -t nat -F
root@Firewall:~#
```

```
root@Firewall:~# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

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
root@Firewall:~#
```

Configuración de reglas de NAT en firewall.

```

root@Firewall:~# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.11
root@Firewall:~# iptables -t nat -A POSTROUTING -s 172.22.229.13 -o eth0 -j MASQUERADE
root@Firewall:~# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination              tcp dpt:http to:192.168.0.11
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  --  172.22.229.13          anywhere
root@Firewall:~#

```

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.11: esta regla redirige todo el tráfico TCP entrante en el puerto 80 de la interfaz eth0 hacia la dirección IP 192.168.0.11.

iptables -t nat -A POSTROUTING -s 172.22.229.13 -o eth0 -j MASQUERADE: esta regla aplica el masquerading al tráfico saliente con origen en la dirección IP 172.22.229.13, enviándolo a través de la interfaz eth0

```

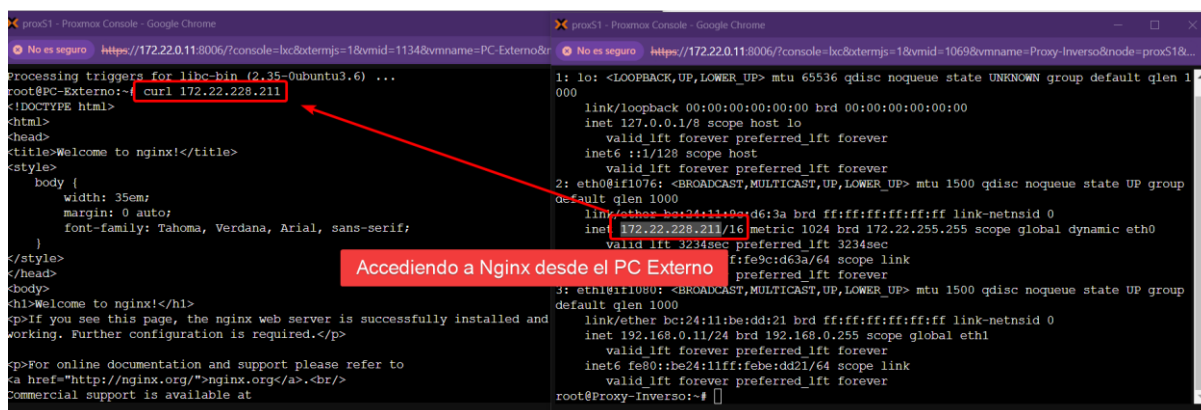
root@Firewall:~# iptables -P INPUT ACCEPT
root@Firewall:~# iptables -P OUTPUT ACCEPT
root@Firewall:~# iptables -p FORWARD ACCEPT
iptables v1.8.7 (nf_tables): unknown protocol "forward" specified
Try `iptables -h' or 'iptables --help' for more information.
root@Firewall:~# iptables -P FORWARD ACCEPT
root@Firewall:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
root@Firewall:~#

```


Accediendo a Nginx desde el PC Externo.



```
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
root@PC-Externo:~# curl 172.22.228.211
<!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
http://nginx.org/</a>.<br/>
Commercial support is available at
```

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
000
    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@i1076: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
default qlen 1000
    link/ether bc:24:11:9c:d6:3a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.22.228.211/16 metric 1024 brd 172.22.255.255 scope global dynamic eth0
        valid_lft 3234sec preferred_lft 3234sec
        fe9c:d63a/64 scope link
        preferred_lft forever
3: eth1@i1080: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group
default qlen 1000
    link/ether bc:24:11:9c:dd:21 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.0.11/24 brd 192.168.0.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:febe:dd21/64 scope link
        valid_lft forever preferred_lft forever
root@Proxy-Inverso:~#
```

Conclusiones

Está siendo una tarea complicada la compresión y práctica de iptables, creo que necesitaría más tiempo y ponerme a mirar teoría para asimilar completamente los conceptos y técnicas de esta práctica, por ello que no esté acabada.

La parte faltante es la parte de dcpdump, que es crucial para capturar el tráfico en la red y determinar si los paquetes están llegando o saliendo correctamente.

Al no emplear tcpdump, no he podido analizar el tráfico de red de manera exhaustiva, lo que podría haberme facilitado identificar posibles errores en la configuración de iptables.