Configuración de iptables para servidor web

M1 con el cortafuegos abierto completamente:

```
  System load:  0.0               Processes:           70
  Usage of /:   6.4% of 19.43GB   Users logged in:     0
  Memory usage: 20%               IP address for eth0: 172.16.169.138
  Swap usage:   0%

  Graph this data and manage this system at https://landscape.canonical.com/

pedro@m1:~$
pedro@m1:~$
pedro@m1:~$ sudo ./reglas_reset.sh
[sudo] password for pedro:
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

pedro@m1:~$
pedro@m1:~$
pedro@m1:~$ _
```

Ahora mismo, estando abierto, Apache sirve el tráfico HTTP y HTTPS:

```
mac:~ pedro$
mac:~ pedro$ curl http://172.16.169.138
<html>
<body>

<h1>Funciona m1 :)</h1>

<p>inicio en el servidor m1
</p>

</body>
</html>
mac:~ pedro$
mac:~ pedro$ curl -k https://172.16.169.138
<html>
<body>

<h1>Funciona m1 :)</h1>

<p>inicio en el servidor m1
</p>

</body>
</html>
mac:~ pedro$
mac:~ pedro$
```

El script para establecer la configuración del cortafuegos para el servidor web:

```
-rwxr-xr-x 1 pedro pedro  429 may  2 22:59 reglas_iptables_set.sh
-rwxr-xr-x 1 pedro pedro  173 abr 22 21:52 reglas_reset.sh
pedro@m1:~$
pedro@m1:~$ cat reglas_iptables_set.sh
#!/bin/sh

 iptables -F
 iptables -X
 iptables -Z
 iptables -t nat -F

 iptables -P INPUT DROP
 iptables -P OUTPUT DROP

 iptables -A INPUT  -i lo -j ACCEPT
 iptables -A OUTPUT -o lo -j ACCEPT

iptables -A INPUT  -i eth0 -p tcp -m multiport --dports 22,80,443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp -m multiport --sports 22,80,443 -m state --state ESTABLISHED -j ACCEPT


 iptables -L -n -v
pedro@m1:~$
pedro@m1:~$
```

Lo ejecutamos y comprobamos el estado del cortafuegos:

```
pedro@m1:~$
pedro@m1:~$ sudo ./reglas_iptables_set.sh
Chain INPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     all  --  lo     *       0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     tcp  --  eth0   *       0.0.0.0/0            0.0.0.0/0
          multiport dports 22,80,443 state NEW,ESTABLISHED

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy DROP 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     all  --  *      lo      0.0.0.0/0            0.0.0.0/0

    0     0 ACCEPT     tcp  --  *      eth0    0.0.0.0/0            0.0.0.0/0
          multiport sports 22,80,443 state ESTABLISHED
pedro@m1:~$
pedro@m1:~$
pedro@m1:~$ _
```

Tras poner la configuración, vemos que sigue sirviendo HTTP y HTTPS:

```
mac:~ pedro$
mac:~ pedro$ curl http://172.16.169.138/pag.html
<html>
<body>

<h1>otro fichero HTML (m1)</h1>

<p>
con otro contenido (m1)
</p>

</body>
</html>
mac:~ pedro$
mac:~ pedro$ curl -k https://172.16.169.138/pag.html
<html>
<body>

<h1>otro fichero HTML (m1)</h1>

<p>
con otro contenido (m1)
</p>

</body>
</html>
mac:~ pedro$
mac:~ pedro$
```