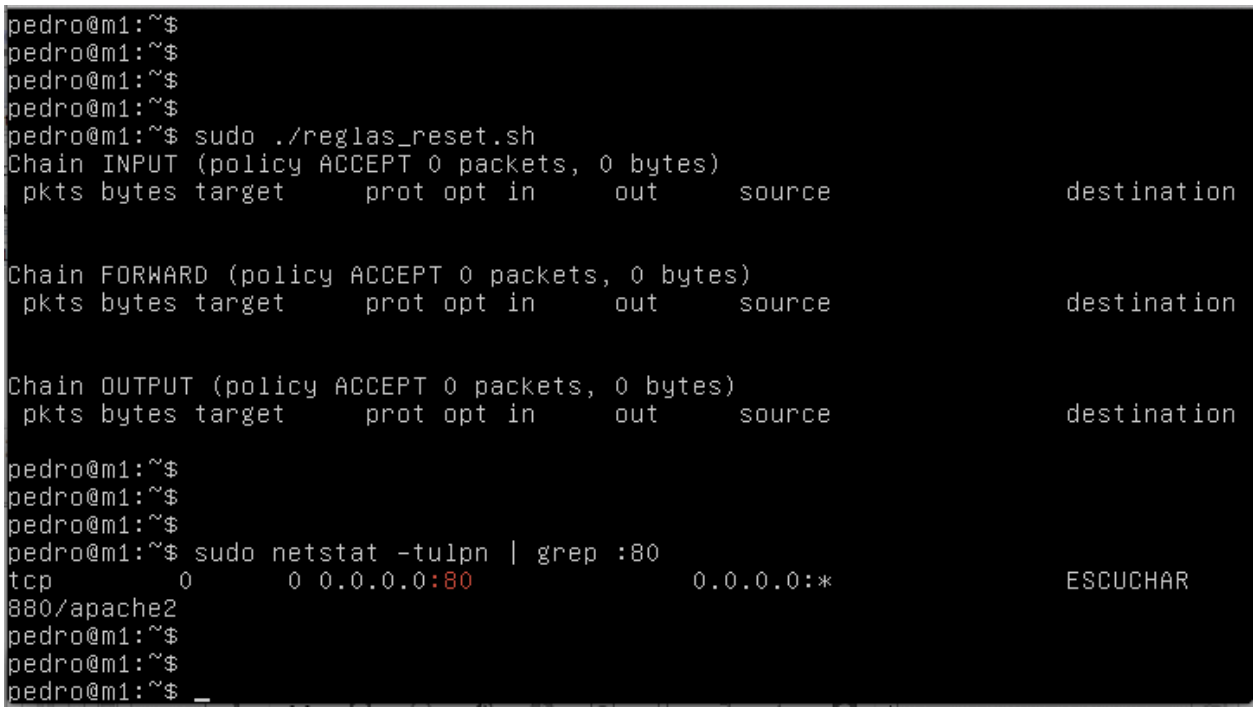
Configurar una máquina cortafuegos externa a los servidores web

Voy a usar las siguientes máquinas:
servidor-web = M1 = 172.16.169.138
cortafuegos = M2 = 172.16.169.137

En la M1 tendremos el servidor web, con Apache funcionando, y puesto que vamos a poner un cortafuegos externo, le pondremos la configuración de iptables por defecto:



En la M2 vamos a configurar el cortafuegos para filtrar el tráfico y a la vez reencaminar el tráfico HTTP hacia el servidor web (M1). Para ello, usaremos el siguiente script:

```
#!/bin/sh

# borrar todas las reglas
iptables -F
iptables -t nat -F
iptables -X
iptables -t nat -X

# política por defecto: bloquearlo todo
iptables -P INPUT DROP
iptables -P OUTPUT DROP

# acceso a localhost
iptables -A INPUT  -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# tráfico SSH
iptables -A INPUT  -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT

# tráfico HTTP
iptables -A INPUT  -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT

# habilitar en el kernel el redireccionamiento
echo 1 > /proc/sys/net/ipv4/ip_forward

# redireccionamiento HTTP
iptables -t nat -A PREROUTING  -p tcp --dport 80 -j DNAT --to-destination 172.16.169.138:80
iptables -t nat -A POSTROUTING -p tcp -d 172.16.169.138 --dport 80 -j SNAT --to-source 172.16.169.137
```

```
pedro@m2:~$ sudo iptables -L -n -v
Chain INPUT (policy DROP 29 packets, 7136 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

   33  2244 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp dpt:80

Chain FORWARD (policy ACCEPT 10 packets, 980 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy DROP 38 packets, 12464 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

   22  3608 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp spt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
          tcp spt:80
pedro@m2:~$ _
```

Si hacemos peticiones a la IP de la M2, veremos que nos sirve la página que hay en el espacio web de la M1, ya que se está redirigiendo el tráfico HTTP:

```
mac:~ pedro$
mac:~ pedro$ curl http://172.16.169.137/pag.html
<html>
<body>

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

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

</body>
</html>
mac:~ pedro$
mac:~ pedro$ curl --connect-timeout 3 https://172.16.169.137/pag.html
curl: (28) Connection timed out after 3003 milliseconds
mac:~ pedro$
mac:~ pedro$ _
```

Y también vemos que el tráfico HTTPS está bloqueado, ya que no hemos configurado las iptables para permitir y redirigir este otro tipo de tráfico.

Sin embargo, en la M1 sí está configurado y funcionando el HTTPS (lo comprobamos haciendo peticiones directas a la IP de la M1):

```
mac:~ pedro$ curl --connect-timeout 3 https://172.16.169.137/pag.html
curl: (28) Connection timed out after 3003 milliseconds
mac:~ pedro$
mac:~ pedro$ curl -k --connect-timeout 3 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$
```