

Índice:

IPTABLES (Linux)	2
1º) Ver la versión de Iptables:	2
2º) Borrado de todas las reglas	2
4º) Eliminar todos los paquetes que entren.	3
5º) Permitir la salida de paquetes.	3
6º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155.	3
7º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección de red 192.168.0.0.	4
8º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155 y enviar un mensaje de error icmp.	4
9º) Permitir conexiones locales (al localhost), por ejemplo, a mysql.	4
10º) Permitir el acceso a nuestro servidor web (puerto TCP 80).....	5
11º) Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).	5
12º) Permitimos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de SSH.....	5
13º) Rechazamos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de Telnet.	5
14º) Rechazamos las conexiones que se originen de la máquina con la dirección física 00:db:f0:34:ab:78. Firewall de una LAN.....	5
15º) Rechazamos todo el tráfico que ingrese a nuestra red LAN 192.168.0.0 /24 desde una red remota, como Internet, a través de la interfaz eth0.	6
16º) Cerramos el rango de puerto bien conocido desde cualquier origen:.....	6
17º) Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80):... 6	6
18º) Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https:	7
19º) Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red:	7
20º) Permitimos enviar y recibir e-mail a todos:	7
21º) Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24:.....	7
22º) Permitimos el paso de un equipo específico 192.168.3.5 a un servicio (puerto 5432) que ofrece un equipo específico (192.168.0.5) y su respuesta:	7
23º) Permitimos el paso de paquetes cuya conexión ya se ha establecido o es nueva pero está relacionada a una conexión ya establecida	8

IPTABLES (Linux)

1º) Ver la versión de Iptables:

Solución:

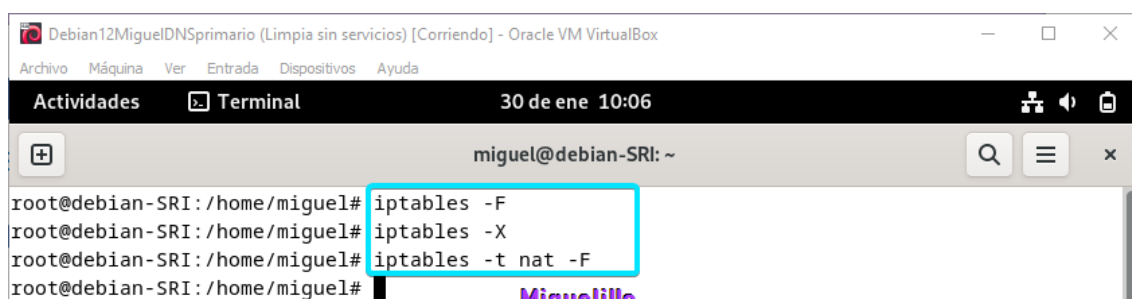


```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 10:01
miguel@debian-SRI: ~
miguel@debian-SRI:~$ sudo iptables --version
iptables v1.8.9 (nf_tables)
miguel@debian-SRI:~$
```

Miguelillo

2º) Borrado de todas las reglas

Solución:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 10:06
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -F
root@debian-SRI:/home/miguel# iptables -X
root@debian-SRI:/home/miguel# iptables -t nat -F
root@debian-SRI:/home/miguel#
```

Miguelillo

iptables -F limpia todas las reglas de filtrado.

iptables -X elimina todas las cadenas personalizadas.

iptables -t nat -F elimina todas las reglas de traducción de direcciones de red en la tabla NAT.

3º) Añadir una regla a la cadena INPUT para aceptar todos los paquetes que se originan desde la dirección 192.168.0.155.

Solución:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 10:10
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j ACCEPT
root@debian-SRI:/home/miguel#
```

Miguelillo

-A INPUT: Agrega (-A) una nueva regla a la cadena de entrada (INPUT).

-s 192.168.0.155: Especifica la dirección IP de origen (source) que debe cumplir la regla.

-j **ACCEPT**: Indica que si un paquete cumple con las condiciones especificadas (en este caso, provenir de la dirección IP 192.168.0.155), se debe aceptar (ACCEPT) el paquete y permitir su paso.

4º) Eliminar todos los paquetes que entren.

Solución:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  30 de ene 10:14
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -j DROP
root@debian-SRI:/home/miguel#
```

-j **DROP**: Especifica que, si un paquete coincide con esta regla, el paquete debe ser descartado (DROP)

5º) Permitir la salida de paquetes.

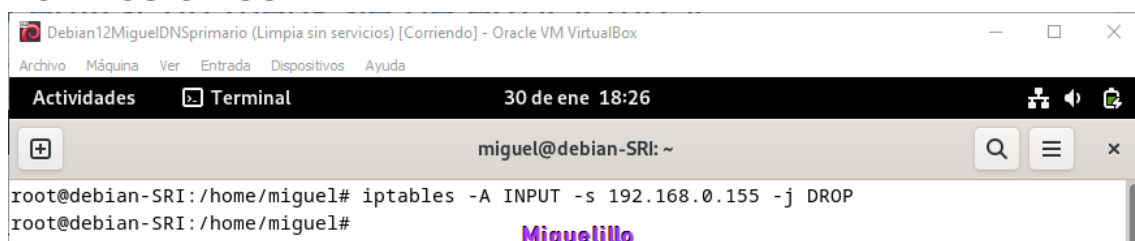
Solución:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  30 de ene 18:01
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A OUTPUT -j ACCEPT
root@debian-SRI:/home/miguel#
```

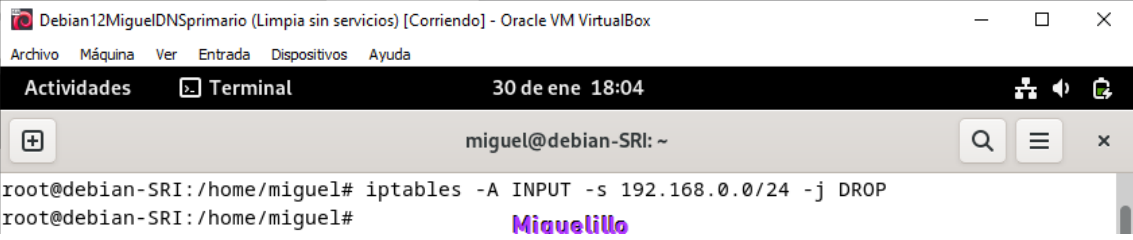
-A **OUTPUT**: Agrega (-A) una nueva regla a la cadena de salida (OUTPUT)

6º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155.



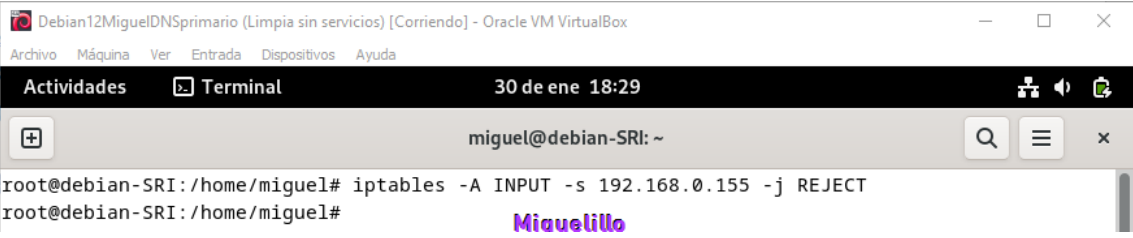
```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Actividades  Terminal  30 de ene 18:26
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j DROP
root@debian-SRI:/home/miguel#
```

7º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección de red 192.168.0.0.



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:04
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.0.0/24 -j DROP
root@debian-SRI:/home/miguel#
```

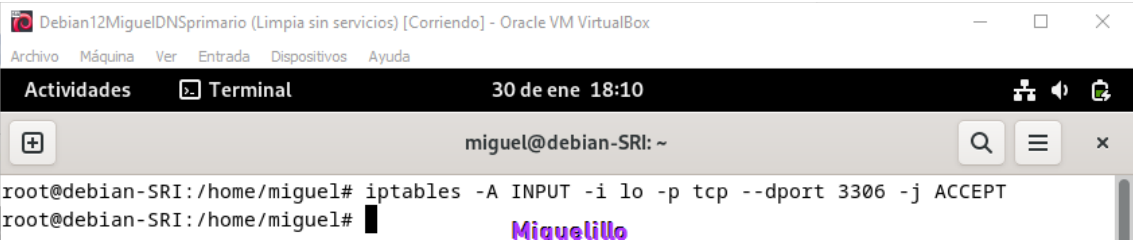
8º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155 y enviar un mensaje de error icmp.



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:29
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.0.155 -j REJECT
root@debian-SRI:/home/miguel#
```

-j REJECT: Indica que si un paquete coincide con esta regla, se debe rechazar (REJECT), es decir, se enviará un mensaje de error al remitente indicando que el acceso está prohibido.

9º) Permitir conexiones locales (al localhost), por ejemplo, a mysql.



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:10
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -i lo -p tcp --dport 3306 -j ACCEPT
root@debian-SRI:/home/miguel#
```

-i lo: Especifica la interfaz de red de entrada. En este caso, se refiere a la interfaz de bucle local (lo), que es utilizada para las comunicaciones internas del propio sistema.

-p tcp: Especifica el protocolo de transporte, que en este caso es TCP

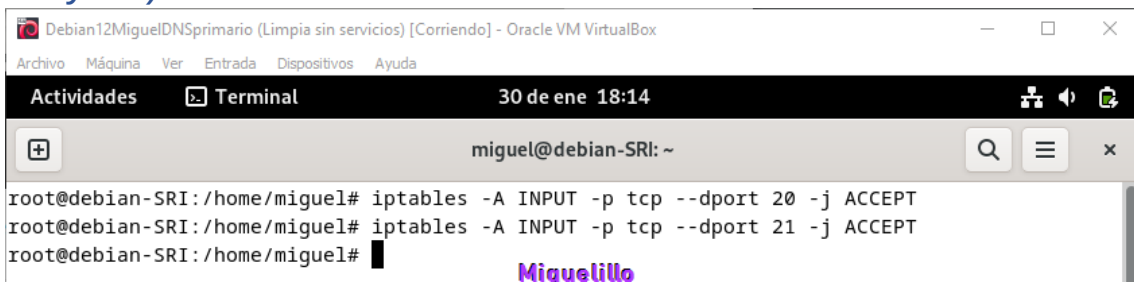
--dport 3306: Indica que la regla se aplica a los paquetes destinados al puerto de destino 3306. Este es el que usa mysql.

10º) Permitir el acceso a nuestro servidor web (puerto TCP 80).



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:11
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
root@debian-SRI:/home/miguel#
```

11º) Permitir el acceso a nuestro servidor ftp (puerto TCP 20 y 21).



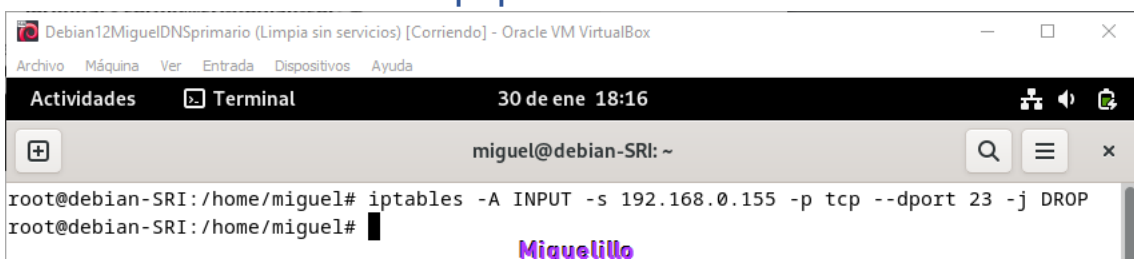
```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:14
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -p tcp --dport 20 -j ACCEPT
root@debian-SRI:/home/miguel# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
root@debian-SRI:/home/miguel#
```

12ª) Permitimos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de SSH.



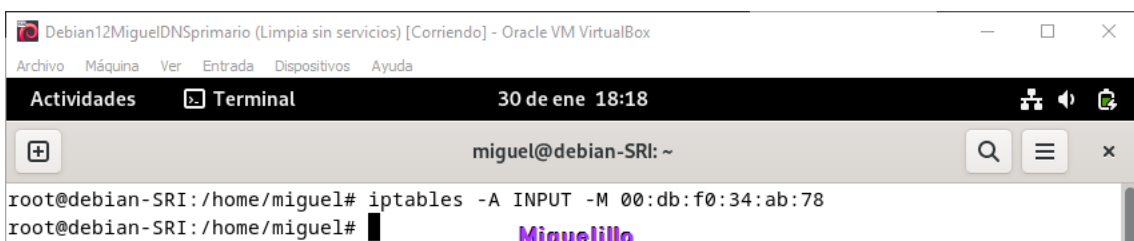
```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:15
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.0.155 -p tcp --dport 22 -j ACCEPT
root@debian-SRI:/home/miguel#
```

13º) Rechazamos a la máquina con IP 192.168.0.155 conectarse a nuestro equipo a través de Telnet.



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:16
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.0.155 -p tcp --dport 23 -j DROP
root@debian-SRI:/home/miguel#
```

14º) Rechazamos las conexiones que se originen de la máquina con la dirección física 00:db:f0:34:ab:78. Firewall de una LAN



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:18
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -M 00:db:f0:34:ab:78
root@debian-SRI:/home/miguel#
```

15º) Rechazamos todo el tráfico que ingrese a nuestra red LAN 192.168.0.0 /24 desde una red remota, como Internet, a través de la interfaz eth0.



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:22
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 0.0.0.0 -i eth0 -d 192.168.0.0/24 -j DROP
root@debian-SRI:/home/miguel#
```

-A FORWARD: se utiliza para el tráfico que se está reenviando a través del sistema, es decir, para el tráfico que no tiene como origen ni destino el propio sistema, sino que está pasando a través de él.

-s 0.0.0.0: La dirección de origen IP 0.0.0.0 no se refiere a una dirección específica, sino que es utilizada para indicar "cualquier dirección" o "cualquier interfaz"

-d 192.168.0.0/24: Esta parte de la regla especifica la dirección de destino (destination) del tráfico

16º) Cerramos el rango de puerto bien conocido desde cualquier origen:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:39
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 0.0.0.0 -p tcp --dport 1:1024 -j DROP
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 0.0.0.0 -p udp --dport 1:1024 -j DROP
root@debian-SRI:/home/miguel#
```

Los puertos bien conocidos generalmente están reservados para servicios estándar. Del 1 al 1024 TCP y UDP

17º) Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80):



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:44
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -p tcp -d 192.168.1.50 --dport 80 -j ACCEPT
root@debian-SRI:/home/miguel#
```

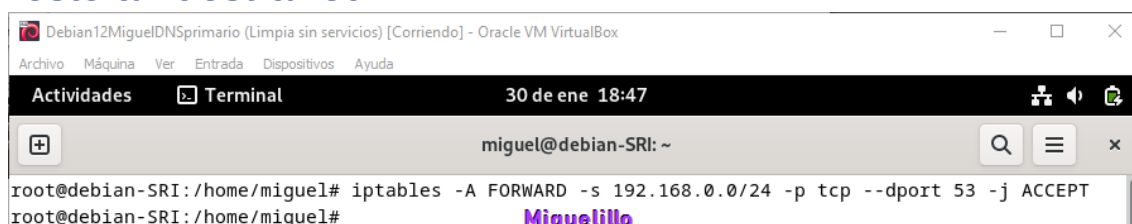
18º) Aceptamos que nuestra LAN 192.168.0.0/24 vayan a puertos https:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:46
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 443 -j ACCEPT
```

Miguelillo

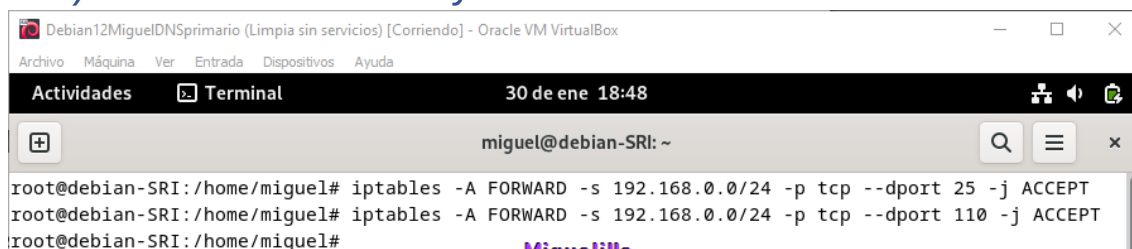
19º) Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:47
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 53 -j ACCEPT
root@debian-SRI:/home/miguel#
```

Miguelillo

20º) Permitimos enviar y recibir e-mail a todos:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:48
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 25 -j ACCEPT
root@debian-SRI:/home/miguel# iptables -A FORWARD -s 192.168.0.0/24 -p tcp --dport 110 -j ACCEPT
root@debian-SRI:/home/miguel#
```

Miguelillo

21º) Cerramos el acceso de una red definida 192.168.3.0/24 a nuestra red LAN 192.168.2.0/24:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:52
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.3.0/24 -d 192.168.2.0 -j DROP
root@debian-SRI:/home/miguel#
```

Miguelillo

22º) Permitimos el paso de un equipo específico 192.168.3.5 a un servicio (puerto 5432) que ofrece un equipo específico (192.168.0.5) y su respuesta:



```
Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 30 de ene 18:53
miguel@debian-SRI: ~
root@debian-SRI:/home/miguel# iptables -A INPUT -s 192.168.3.5 -d 192.168.0.5 -p tcp --dport 5432 -j ACCEPT
root@debian-SRI:/home/miguel#
```

Miguelillo

23º) Permitimos el paso de paquetes cuya conexión ya se ha establecido o es nueva pero está relacionada a una conexión ya establecida

A screenshot of a terminal window titled "Debian12MiguelDNSprimario (Limpia sin servicios) [Corriendo] - Oracle VM VirtualBox". The terminal shows the command `iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT` being executed. The prompt is `root@debian-SRI:/home/miguel#`. The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". The title bar shows "30 de ene 19:01". The terminal output shows the command being executed and a cursor on the next line.

```
root@debian-SRI:/home/miguel# iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
root@debian-SRI:/home/miguel#
```

-m state --state ESTABLISHED,RELATED: Utiliza el módulo "state" para especificar el estado de la conexión. En este caso, la regla permite el tráfico que está en el estado "ESTABLISHED" (establecido) o "RELATED" (relacionado). Esto incluye, por ejemplo, respuestas a conexiones salientes establecidas previamente y tráfico relacionado con conexiones ya establecidas.