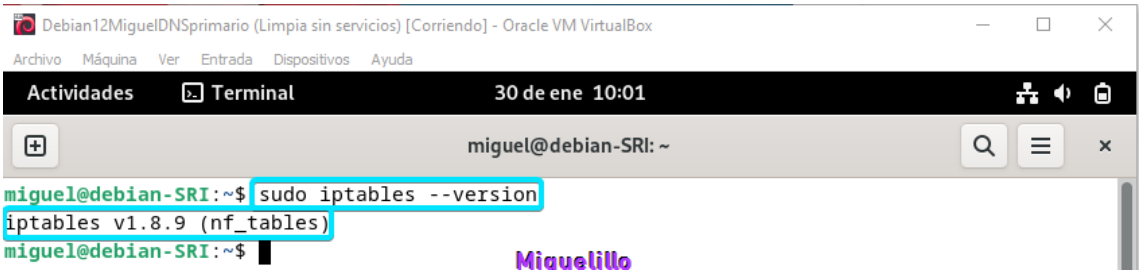
Índice:

IPTABLES (Linux)

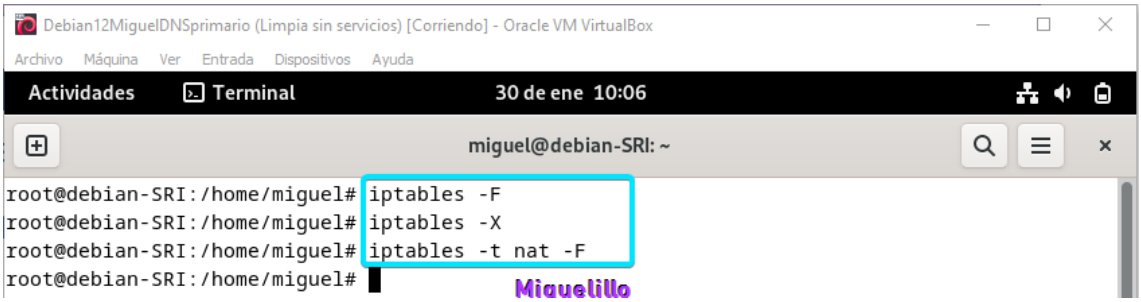
1º) Ver la versión de Iptables:

Solución:



2º) Borrado de todas las reglas

Solución:



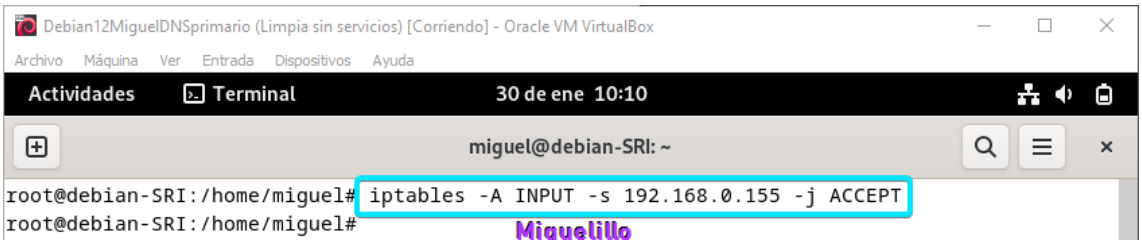
iptables -F limpia todas las reglas de filtrado.

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:



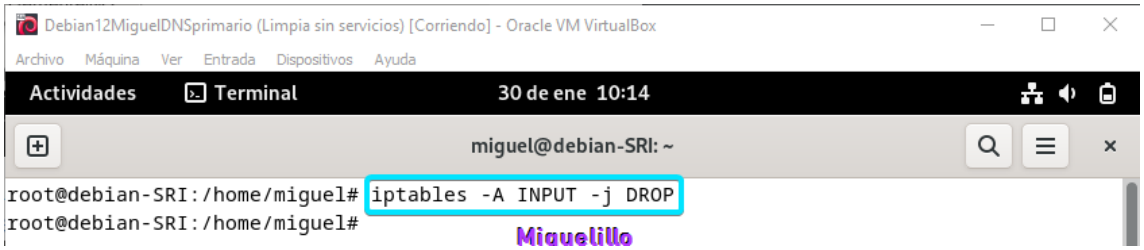
-A INPUT: Agrega (-A) una nueva regla a la cadena de entrada (INPUT).

-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:



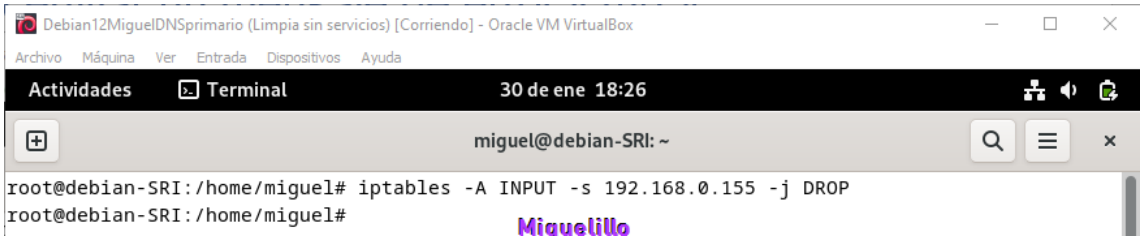
-j DROP: Especifica que, si un paquete coincide con esta regla, el paquete debe ser descartado (DROP)

5º) Permitir la salida de paquetes.

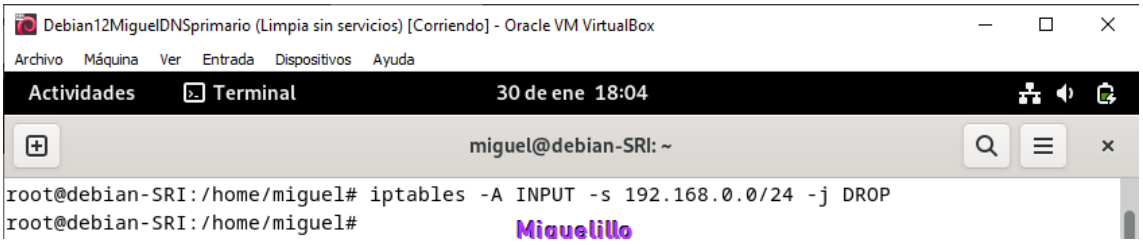
Solución:

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

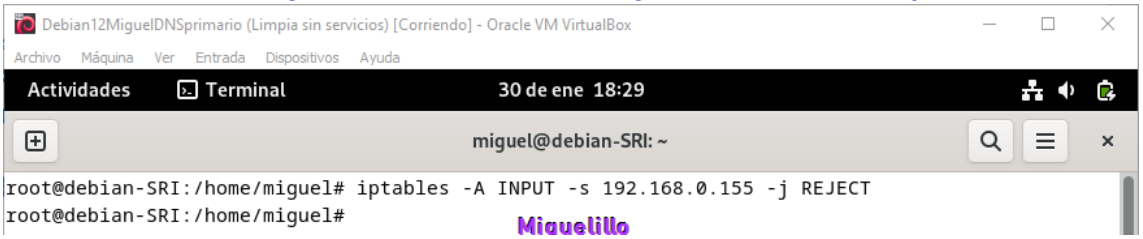
6º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155.



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.

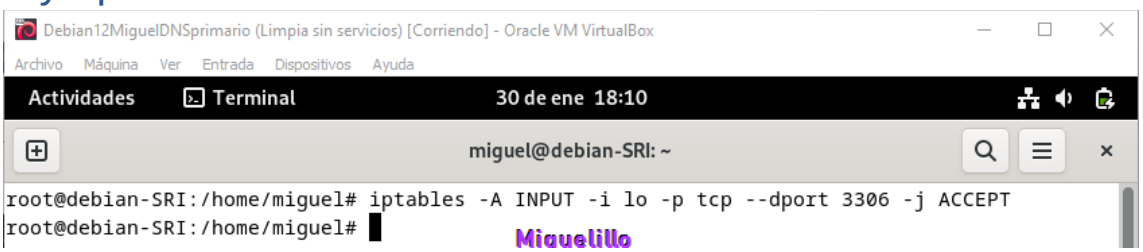


8º) Añadir una regla a la cadena INPUT para rechazar todos los paquetes que se originan desde la dirección 192.168.0.155 y enviar un mensaje de error icmp.



-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.



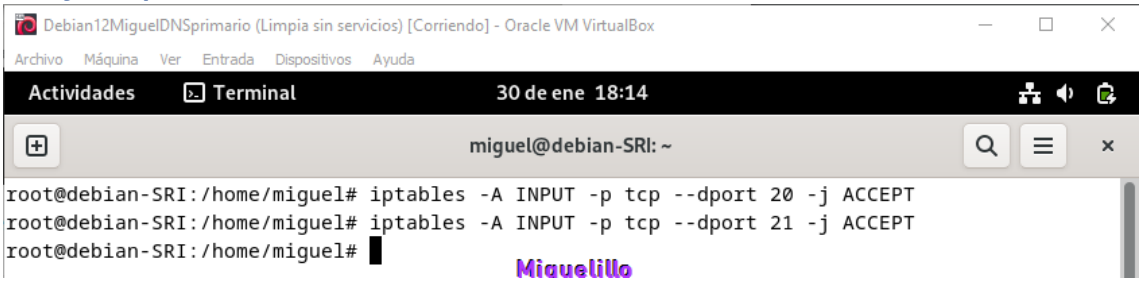
-i lo: Especifica la interfaz de red de entrada. En este caso, se refiere a la interfaz de bucle local (lo), que es utilizada para las comunicaciones internas del propio sistema.

-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).

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



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

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

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

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.

-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:

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

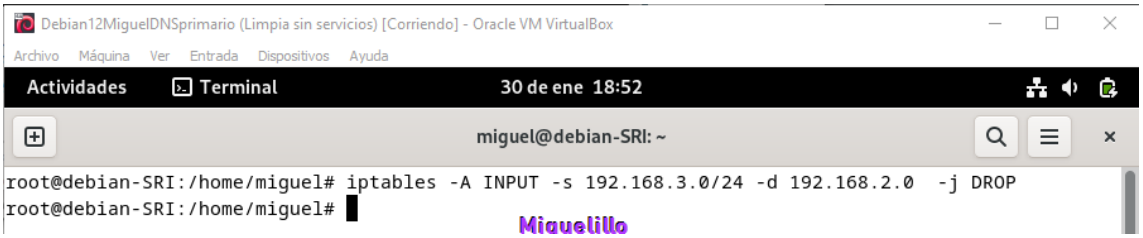
17º) Aceptamos que vayan de nuestra red 192.168.0.0/24 a un servidor web (puerto 80):

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

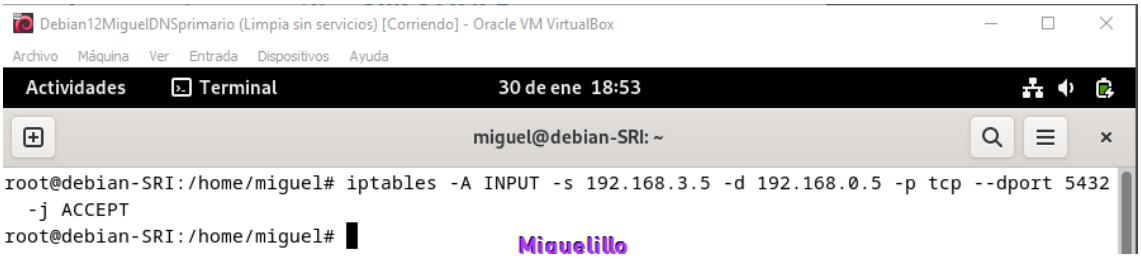
19º) Aceptamos que los equipos de nuestra red LAN 192.168.0.0/24 consulten los DNS, y denegamos todo el resto a nuestra red:

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

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



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:



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

-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.