
Administración de Sistemas



Actividad en clase 3

Netfilter

08/11/2021

Marcos Eladio Somoza Corral

21711787

ÍNDICE

| | |
|--|---|
| 1. Aceptar las conexiones entrantes al puerto TCP 5432. | 4 |
| 3. Eliminar todas las reglas anteriores. | 4 |
| 4. Denegar en modo silencioso todas las conexiones entrantes de la red 10.0.4.0/30 al puerto TCP 22. | 4 |
| 5. Aceptar todas las conexiones entrantes de la interfaz de loopback. | 4 |
| 6. Aceptar las conexiones entrantes al puerto TCP 5432. | 4 |
| 7. Permitir las conexiones entrantes para el servicio LDAP utilizando el puerto por defecto. | 5 |
| 8. Guardar la configuración de forma permanente. | 5 |
| 9. Denegar el acceso al puerto SSH desde cualquier origen. | 5 |
| 10. Permitir el acceso al puerto por defecto de MySQL para la ip 192.168.1.5. | 6 |

1. Aceptar las conexiones entrantes al puerto TCP 5432.

Utilizando el comando ***iptables -A INPUT -p tcp --dport 5432 -j ACCEPT*** permitiremos conexiones entrantes del protocolo tcp por el puerto 5432.

2. Denegar por defecto todas las conexiones del tipo FORWARD.

Usando el comando ***iptables -P FORWARD REJECT*** asignamos forward como política predeterminada, además de denegar por defecto todas sus conexiones.

3. Eliminar todas las reglas anteriores.

Con el comando ***iptables --flush*** borraríamos todas las reglas. Cabe destacar que también se pueden utilizar el comando ***iptables -F***.

4. Denegar en modo silencioso todas las conexiones entrantes de la red 10.0.4.0/30 al puerto TCP 22.

Usando el comando ***iptables -P INPUT -s 10.0.4.0/30 -p tcp --dport 22*** denegaremos en modo silencioso (DROP) las conexiones entrantes (-A INPUT) de la red (-s 10.0.4.0/30) al puerto 22 (-dport 22) del protocolo TCP (-p tcp).

5. Aceptar todas las conexiones entrantes de la interfaz de loopback.

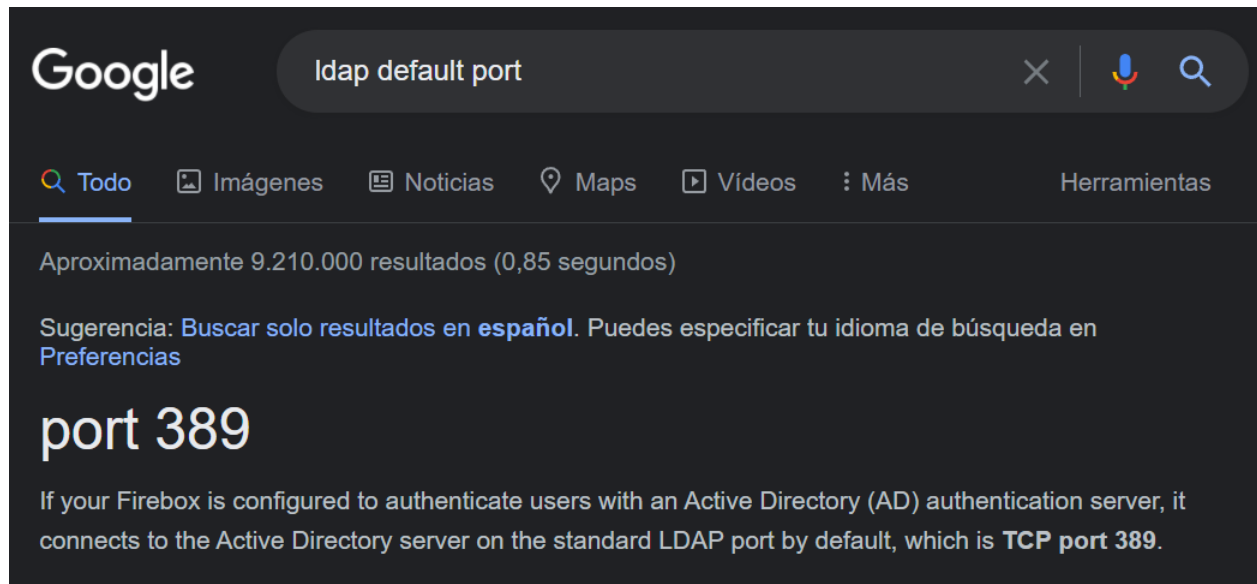
Gracias a este comando ***iptables -A INPUT -i lo -j ACCEPT*** agregamos la especificación de entrada a la cadena (-A), la interfaz de loopback con (-i lo) e identificamos el objetivo de aceptarla (-j ACCEPT).

6. Aceptar las conexiones entrantes al puerto TCP 5432.

Utilizando el comando ***iptables -A INPUT -p tcp --dport 5432 -j ACCEPT*** permitiremos conexiones entrantes del protocolo tcp por el puerto 5432.

7. Permitir las conexiones entrantes para el servicio LDAP utilizando el puerto por defecto.

Para poder permitir las conexiones entrantes para el servicio LDAP (usando el puerto por defecto), se debe saber de qué puerto se trata; con una rápida búsqueda en Google se soluciona:



Así pues, el comando sería ***iptables -A INPUT -p tcp --dport 389 -j ACCEPT***, igual que el apartado anterior pero con el puerto correcto.

8. Guardar la configuración de forma permanente.

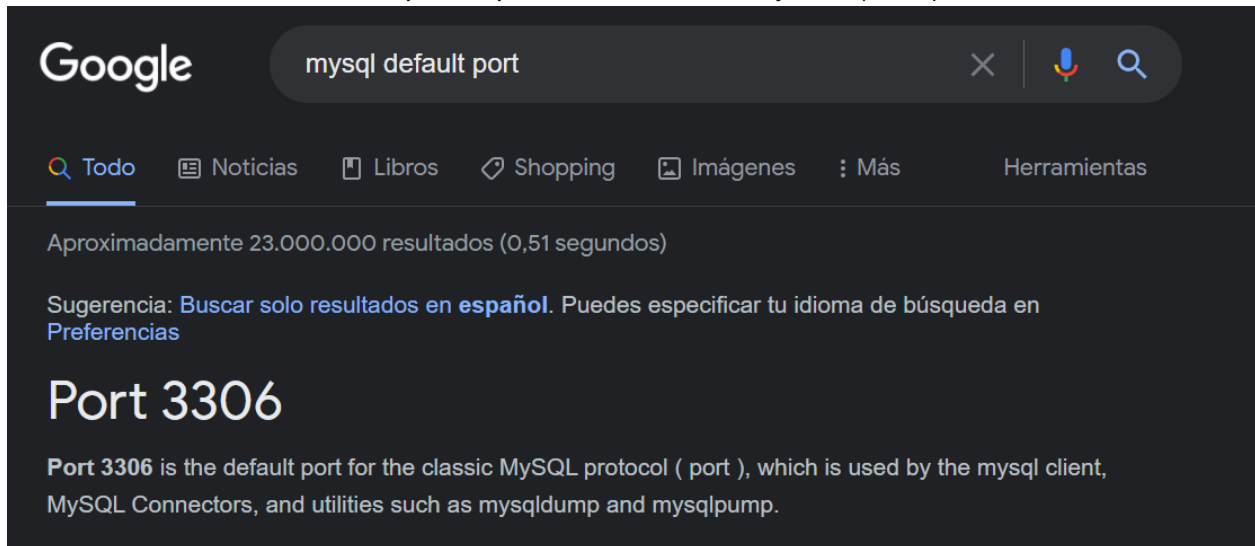
Para guardar la configuración de nuestro **netfilter** de forma permanente se debe hacer uso del comando ***iptables-save***, y, como se ha visto en entregas anteriores (*crontab log file*), se deberá guardar el output del comando en un directorio determinado. Así pues, el comando completo sería ***iptables-save > /root/dsl.fw*** (siendo ***/root/dsl.fw*** el directorio de guardado).

9. Denegar el acceso al puerto SSH desde cualquier origen.

El puerto predeterminado de las conexiones **ssh** es el 22, así pues, y teniendo en cuenta de que se trata de una conexión **tcp**, el comando sería tal que ***iptables -I INPUT -p tcp --dport 22 -j REJECT***, se debe recordar que se usa **REJECT** en lugar de **DROP** porque no pide que sea un bloqueo silencioso.

10. Permitir el acceso al puerto por defecto de MySQL para la ip 192.168.1.5.

De nuevo, se debe conocer el puerto predeterminado de MySQL (3306).



Y aplicarlo teniendo en cuenta que se deberá usar -s para asignar el host de origen : ***iptables -A INPUT -s 192.168.1.5 -p tcp --dport 3306.***