



**Título de la actividad: IPTABLES –
CONFIGURACIÓN Y ANÁLISIS DE REGLAS**

Nombre: Eric Carmen Soto

Fecha de realización: 09/10/2025

Semestre: 9no

Unidad de Aprendizaje (UA): Sistemas Operativos

Periodo escolar: 2025B

Institución: Centro Universitario UAEM
Zumpango

1. Mostrar las reglas de IPTABLES antes de iniciar la actividad

Comando utilizado:

sudo iptables -L -v

Descripción:

Este comando lista todas las reglas activas en las cadenas INPUT, OUTPUT y FORWARD, mostrando detalles como el número de paquetes y bytes procesados.

```
ericc@Kareli: ~$ sudo iptables -L -v
[sudo] password for ericc:
Chain INPUT (policy ACCEPT 162 packets, 12636 bytes)
pkts bytes target prot opt in out source destination
0 0 35613 ufw-before-logging-input all -- any anywhere anywhere
0 0 35613 ufw-before-input all -- any anywhere anywhere
0 0 35613 ufw-after-logging-input all -- any anywhere anywhere
0 0 35613 ufw-after-input all -- any anywhere anywhere
0 0 35613 ufw-reject-input all -- any anywhere anywhere
0 0 35613 ufw-track-input all -- any anywhere anywhere
0 0 ACCEPT all -- eth1 any anywhere
0 0 DROP all -- eth1 any anywhere
0 0 REJECT all -- eth1 any anywhere reject-with icmp-port-unreachable
129 13416 ACCEPT all -- eth0 any anywhere state RELATED,ESTABLISHED
0 0 ACCEPT all -- eth0 any anywhere state RELATED,ESTABLISHED
0 0 ACCEPT all -- eth1 any anywhere
132 9561 ACCEPT all -- lo any anywhere
0 0 ACCEPT tcp -- any any anywhere tcp dpt:smtp flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:http flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:https flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:ssh flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere tcp dpt:images flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT udp -- eth1 any anywhere
0 0 ACCEPT udp -- any any 200.33.146.217 anywhere
0 0 DROP tcp -- any any anywhere tcp dpt:ssh
0 0 DROP udp -- any any anywhere udp dpt:23

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ufw-before-logging-forward all -- any anywhere anywhere
0 0 ufw-before-forward all -- any anywhere anywhere
0 0 ufw-after-logging-forward all -- any anywhere anywhere
0 0 ufw-after-forward all -- any anywhere anywhere
0 0 ufw-reject-forward all -- any anywhere anywhere
0 0 ACCEPT all -- eth1 eth0 anywhere anywhere
0 0 ACCEPT all -- eth0 eth1 anywhere anywhere state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 276 packets, 21641 bytes)
pkts bytes target prot opt in out source destination
276 21641 ufw-before-logging-output all -- any anywhere anywhere
276 21641 ufw-before-output all -- any anywhere anywhere
276 21641 ufw-after-logging-output all -- any anywhere anywhere
276 21641 ufw-after-output all -- any anywhere anywhere
276 21641 ufw-reject-output all -- any anywhere anywhere
276 21641 ufw-track-output all -- any anywhere anywhere
```

2. Crear dos reglas diferentes en IPTABLES

Regla 1: Permitir tráfico HTTP entrante

Comando:

```
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

Descripción:

Esta regla permite el tráfico entrante por el puerto 80 (HTTP), utilizado por servidores web.

Evidencia regla 1

```
ericc@Karer: ~  
ericc@Karer:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
ericc@Karer:~$ sudo iptables -L -v  
Chain INPUT (policy ACCEPT 168 packets, 13104 bytes)  
pkts bytes target prot opt in out source destination  
434 36446 ufw-before-logging-input all -- any any anywhere anywhere  
434 36446 ufw-before-input all -- any any anywhere anywhere  
434 36446 ufw-after-input all -- any any anywhere anywhere  
434 36446 ufw-after-logging-input all -- any any anywhere anywhere  
434 36446 ufw-reject-input all -- any any anywhere anywhere  
434 36446 ufw-track-input all -- any any anywhere anywhere  
0 0 ACCEPT all -- eth1 any anywhere anywhere  
0 0 DROP all -- eth1 any anywhere anywhere  
0 0 REJECT all -- eth1 any anywhere anywhere reject-with icmp-port-unreachable  
129 13416 ACCEPT all -- eth0 any anywhere anywhere state RELATED,ESTABLISHED  
0 0 ACCEPT all -- eth0 any anywhere anywhere state RELATED,ESTABLISHED  
0 0 ACCEPT all -- eth1 any anywhere anywhere  
137 9926 ACCEPT all -- lo any anywhere anywhere  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:smtp flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:https flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:pop3 flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:pop3s flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:imap2 flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:imaps flags:FIN, SYN, RST, ACK/SYN  
0 0 ACCEPT udp -- eth1 any anywhere anywhere udp spt:bootpc dpt:bootps  
0 0 ACCEPT udp -- any any 200.33.146.217 anywhere udp spt:domain  
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:ssh  
0 0 DROP udp -- any any 200.33.146.217 anywhere udp dpt:23  
0 0 DROP all -- any any 200.33.146.217 anywhere  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
0 0 ufw-before-logging-forward all -- any any anywhere anywhere  
0 0 ufw-before-forward all -- any any anywhere anywhere  
0 0 ufw-after-forward all -- any any anywhere anywhere  
0 0 ufw-after-logging-forward all -- any any anywhere anywhere  
0 0 ufw-reject-forward all -- any any anywhere anywhere reject-with icmp-port-unreachable  
0 0 ufw-track-forward all -- any any anywhere anywhere state RELATED,ESTABLISHED  
0 0 ACCEPT all -- eth1 eth0 anywhere anywhere  
0 0 ACCEPT all -- eth0 eth1 anywhere anywhere  
Chain OUTPUT (policy ACCEPT 285 packets, 22310 bytes)  
pkts bytes target prot opt in out source destination
```

Regla 2: Bloquear tráfico SSH en FORWARD

Comando:

sudo iptables -A FORWARD -p tcp --dport 22 -j DROP

Descripción:

Esta regla bloquea el reenvío de paquetes TCP destinados al puerto 22 (SSH). Es útil cuando el equipo actúa como router o puente entre redes, y se desea impedir que el tráfico SSH pase a través de él.

Evidencia regla 2

```
ericc@Karari:~$ sudo iptables -A FORWARD -p tcp --dport 22 -j DROP
ericc@Karari:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 228 packets, 18998 bytes)
pkts bytes target prot opt in out source destination
538 45854 ufw-before-logging-input all -- any any anywhere anywhere
538 45854 ufw-before-input all -- any any anywhere anywhere
538 45854 ufw-after-logging-input all -- any any anywhere anywhere
538 45854 ufw-reject-input all -- any any anywhere anywhere
538 45854 ufw-track-input all -- any any anywhere anywhere
0 0 ACCEPT all -- eth1 any anywhere anywhere
0 0 DROP all -- eth1 any anywhere anywhere
0 0 REJECT all -- eth1 any anywhere anywhere reject-with icmp-port-unreachable
139 14888 ACCEPT all -- eth0 any anywhere anywhere state RELATED,ESTABLISHED
0 0 ACCEPT all -- eth0 any anywhere anywhere state RELATED,ESTABLISHED
0 0 ACCEPT all -- eth1 any anywhere anywhere
171 12974 ACCEPT all -- lo any anywhere anywhere
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:smtp flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:https flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:imaps flags:FIN,SYN,RST,ACK/SYN
0 0 ACCEPT udp -- eth1 any anywhere anywhere udp spt:bootpc dpt:bootps
0 0 ACCEPT udp -- any any nsexd.uninet.net.mx anywhere udp dpt:domain
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:ssh
0 0 DROP all -- any any nsexd.uninet.net.mx anywhere
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target prot opt in out source destination
0 0 ufw-before-logging-forward all -- any any anywhere anywhere
0 0 ufw-before-forward all -- any any anywhere anywhere
0 0 ufw-after-logging-forward all -- any any anywhere anywhere
0 0 ufw-reject-forward all -- any any anywhere anywhere
0 0 ufw-track-forward all -- any any anywhere anywhere
0 0 ACCEPT all -- eth1 eth0 anywhere anywhere state RELATED,ESTABLISHED
0 0 ACCEPT all -- eth0 eth1 anywhere anywhere
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:ssh

Chain OUTPUT (policy ACCEPT 333 packets, 26222 bytes)
pkts bytes target prot opt in out source destination
333 26222 ufw-before-logging-output all -- any any anywhere anywhere
333 26222 ufw-before-output all -- any any anywhere anywhere
333 26222 ufw-after-output all -- any any anywhere anywhere
333 26222 ufw-after-logging-output all -- any any anywhere anywhere
333 26222 ufw-reject-output all -- any any anywhere anywhere
333 26222 ufw-track-output all -- any any anywhere anywhere
0 0 ACCEPT all -- any eth1 anywhere anywhere state RELATED,ESTABLISHED
0 0 DROP all -- any any nsexd.uninet.net.mx anywhere

Chain ufw-after-forward (1 references)
```

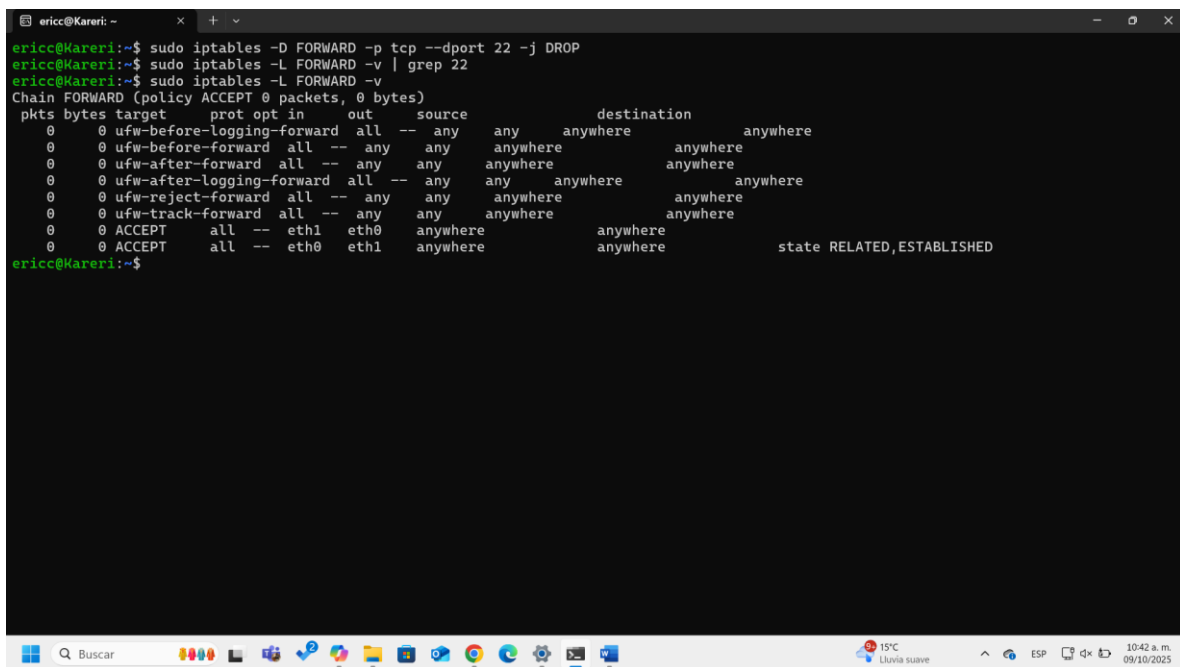
3. Eliminar una de las reglas creadas (regla 2)

Comando:

sudo iptables -D FORWARD -p tcp --dport 22 -j DROP

Descripción:

Se elimina la regla que bloqueaba el tráfico SSH en tránsito por el puerto 22. Esto permite nuevamente el reenvío de paquetes SSH entre interfaces, útil si el equipo actúa como router o puente.



```
ericc@Kareri: ~  
ericc@Kareri:~$ sudo iptables -D FORWARD -p tcp --dport 22 -j DROP  
ericc@Kareri:~$ sudo iptables -L FORWARD -v | grep 22  
ericc@Kareri:~$ sudo iptables -L FORWARD -v  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target      prot opt in     out     source            destination  
  0      0 ufw-before-logging-forward all -- -- any      any      anywhere          anywhere  
  0      0 ufw-before-forward all -- -- any      any      anywhere          anywhere  
  0      0 ufw-after-forward all -- -- any      any      anywhere          anywhere  
  0      0 ufw-after-logging-forward all -- -- any      any      anywhere          anywhere  
  0      0 ufw-reject-forward all -- -- any      any      anywhere          anywhere  
  0      0 ufw-track-forward all -- -- any      any      anywhere          anywhere  
  0      0 ACCEPT all -- eth1   eth0    anywhere          anywhere  
  0      0 ACCEPT all -- eth0   eth1    anywhere          anywhere          state RELATED,ESTABLISHED  
ericc@Kareri:~$
```

4. Mostrar las reglas actuales en IPTABLES

Comando:

sudo iptables -L -v

Descripción:

Se verifica que la regla eliminada ya no aparece (la regla 2) y que la regla de HTTP sigue activa.

```
ericc@Kareni: ~  
ericc@Kareni:~$ sudo iptables -L -v  
Chain INPUT (policy ACCEPT 228 packets, 18800 bytes)  
pkts bytes target prot opt in out source destination  
559 46734 ufw-before-logging-input all -- any any anywhere anywhere  
559 46734 ufw-before-input all -- any any anywhere anywhere  
559 46734 ufw-after-input all -- any any anywhere anywhere  
559 46734 ufw-after-logging-input all -- any any anywhere anywhere  
559 46734 ufw-reject-input all -- any any anywhere anywhere  
559 46734 ufw-track-input all -- any any anywhere anywhere  
0 0 ACCEPT all -- eth1 any anywhere anywhere  
0 0 DROP all -- eth1 any anywhere anywhere  
0 0 REJECT all -- eth1 any anywhere anywhere reject-with icmp-port-unreachable  
154 15220 ACCEPT all -- eth0 any anywhere anywhere state RELATED,ESTABLISHED  
0 0 ACCEPT all -- eth0 any anywhere anywhere state RELATED,ESTABLISHED  
0 0 ACCEPT all -- eth1 any anywhere anywhere  
177 13514 ACCEPT all -- lo any anywhere anywhere  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:smtp flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:https flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:ssh flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:imaps flags:FIN,SYN,RST,ACK/SYN  
0 0 ACCEPT udp -- any any nsnet4.uninet.net.mx anywhere udp spt:bootpc dpt:bootps  
0 0 DROP tcp -- any any anywhere anywhere tcp dpt:ssh  
0 0 DROP udp -- any any anywhere anywhere udp dpt:23  
0 0 DROP all -- any any nsnet4.uninet.net.mx anywhere  
0 0 ACCEPT tcp -- any any anywhere anywhere tcp dpt:http  
  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
0 0 ufw-before-logging-forward all -- any any anywhere anywhere  
0 0 ufw-before-forward all -- any any anywhere anywhere  
0 0 ufw-after-forward all -- any any anywhere anywhere  
0 0 ufw-after-logging-forward all -- any any anywhere anywhere  
0 0 ufw-reject-forward all -- any any anywhere anywhere  
0 0 ufw-track-forward all -- any any anywhere anywhere  
0 0 ACCEPT all -- eth1 eth0 anywhere anywhere state RELATED,ESTABLISHED  
  
Chain OUTPUT (policy ACCEPT 354 packets, 27902 bytes)  
pkts bytes target prot opt in out source destination  
354 27902 ufw-before-logging-output all -- any any anywhere anywhere
```

5. Describir qué acciones realiza ACCEPT, DROP y RETURN en IPTABLES

ACCEPT:

Permite el paso del paquete según la regla definida. El tráfico continúa su curso.

DROP:

Descarta el paquete sin enviar respuesta al origen. Es útil para bloquear tráfico sin revelar información.

RETURN:

Finaliza la evaluación de reglas en una cadena personalizada y regresa al flujo anterior. Se usa en cadenas definidas por el usuario.

REFERENCIAS

[1] "iptables: configuración del firewall en Linux con iptables," RedesZone, [En línea]. Disponible en: <https://www.redeszone.net/gnu-linux/iptables-configuracion-del-firewall-en-linux-con-iptables/>. [Accedido: 09-oct-2025].

[2] "iptables(8) - Linux man page," Linux Die.net, [En línea]. Disponible en: <https://linux.die.net/man/8/iptables>. [Accedido: 09-oct-2025].

[3] "iptables - ArchWiki," Arch Linux Wiki, [En línea]. Disponible en: <https://wiki.archlinux.org/title/Iptables>. [Accedido: 09-oct-2025].

[4] "iptables-persistent," Ubuntu Manpages, [En línea]. Disponible en: <https://manpages.ubuntu.com/manpages/focal/en/man8/iptables-persistent.8.html>. [Accedido: 09-oct-2025].