



**Universidad Autónoma del Estado de México**

**UAEM Zumpango**

**Ingeniería en Computación**

**Unidad de Aprendizaje:**

**Sistemas Operativos**

**Actividad:**

**IPTABLES**

**Alumno:**

**Rodríguez Estudillo Jose Antonio**

**Fecha:**

**09 Octubre de 2025**

## 1. Muestrame las reglas IPTABLES.

```
joseantoniore@JoseToni: ~$ sudo iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- anywhere anywhere
DROP all -- anywhere anywhere
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere
ACCEPT tcp -- anywhere anywhere tcp dpt:smtp flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:http flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:https flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:imap flags:FIN,SYN,RST,ACK/SYN
ACCEPT udp -- anywhere anywhere udp spt:bootpc dpt:bootps
ACCEPT udp -- nsmex4.uninet.net.mx anywhere udp spt:domain
DROP tcp -- anywhere anywhere tcp dpt:ssh
DROP udp -- anywhere anywhere udp dpt:23

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
REJECT all -- 192.168.0.0/24 customer-200-33-145-217.uninet-ide.com.mx reject-with icmp-port-unreachable
joseantoniore@JoseToni: ~$
```

## 2. Cree dos reglas diferentes en IPTABLES.

### 2.1. Describa que hace cada una de estas reglas.

**Regla 1: `sudo iptables -A INPUT -s 192.168.100.50 -j DROP`** (Esta regla va a descartar silenciosamente todos los paquetes que vengan de la dirección IP 192.168.100.50).

**-A INPUT:** Añade (Append) la regla a la cadena INPUT. La cadena INPUT controla todo el tráfico que entra a tu máquina.

**-s 192.168.100.50:** Especifica el origen (source) del tráfico. En este caso, la IP que queremos bloquear.

**-j DROP:** Es la acción (jump) a realizar. DROP significa "descartar" el paquete. El remitente nunca recibe una respuesta, simplemente el paquete se pierde.

**Regla 2: `sudo iptables -A INPUT -p tcp --dport 80 -j DROP`** (Esta regla bloqueará todas las conexiones entrantes que intenten acceder al puerto 80, que es el puerto estándar para el tráfico web HTTP).

- A INPUT:** De nuevo, añadimos la regla a la cadena de tráfico entrante.
- p tcp:** Especifica el **protocolo** (protocol) que estamos filtrando, en este caso, TCP.
- dport 80:** Especifica el **puerto de destino** (destination port) que es el 80 (HTTP).
- j DROP:** La acción es descartar el paquete.

2.2. Acompañé con la captura de los comandos utilizados para crear las reglas.

```
joseantonio@JoseToni:~$ sudo iptables -A INPUT -s 192.168.100.50 -j DROP
[sudo] password for joseantonio:
joseantonio@JoseToni:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
joseantonio@JoseToni:~$
```

3. Muestre nuevamente las reglas de IPTABLES, donde identifique las nuevas reglas creadas anteriormente.

```
joseantonio@JoseToni:~$ sudo iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ACCEPT all -- anywhere anywhere
DROP all -- anywhere anywhere
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere
ACCEPT tcp -- anywhere anywhere tcp dpt:smtp flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:http flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:https flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
ACCEPT tcp -- anywhere anywhere tcp dpt:imap flags:FIN,SYN,RST,ACK/SYN
ACCEPT udp -- anywhere anywhere udp spt:bootpc dpt:bootps
ACCEPT udp -- nsx4.uninet.net.mx anywhere udp spt:domain
DROP tcp -- anywhere anywhere tcp dpt:ssh
DROP udp -- anywhere anywhere udp dpt:23
DROP all -- 192.168.100.50 anywhere
DROP tcp -- anywhere anywhere tcp dpt:http

Chain FORWARD (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- anywhere anywhere state RELATED,ESTABLISHED
REJECT all -- 192.168.0.0/24 customer-200-33-145-217.uninet-ide.com.mx reject-with icmp-port-unreachable
joseantonio@JoseToni:~$
```

#### 4. Elimine de las reglas creadas.

```
joseantoniore@JoseToni: ~$ sudo iptables -D INPUT -p tcp --dport 80 -j DROP
[sudo] password for joseantoniore:
joseantoniore@JoseToni: ~$
```

#### 5. Muestre las reglas en IPTABLES

```
joseantoniore@JoseToni: ~$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere
DROP        all  --  anywhere               anywhere
ACCEPT     all  --  anywhere               anywhere    state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere    state RELATED,ESTABLISHED
ACCEPT     all  --  anywhere               anywhere
ACCEPT     all  --  anywhere               anywhere
ACCEPT     all  --  anywhere               anywhere
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:smtp flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:http flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:https flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:ssh flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:pop3 flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:pop3s flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:imap2 flags:FIN,SYN,RST,ACK/SYN
ACCEPT     tcp  --  anywhere               anywhere    tcp dpt:imaps flags:FIN,SYN,RST,ACK/SYN
ACCEPT     udp  --  anywhere               anywhere    udp spt:bootpc dpt:bootps
ACCEPT     udp  --  ns.mex4.uninet.net.mx  anywhere    udp spt:domain
DROP        tcp  --  anywhere               anywhere    tcp dpt:ssh
DROP        udp  --  anywhere               anywhere    udp dpt:23
DROP        all  --  192.168.100.50         anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere
ACCEPT     all  --  anywhere               anywhere    state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     all  --  anywhere               anywhere    state RELATED,ESTABLISHED
REJECT     all  --  192.168.0.0/24         customer-200-33-145-217.uninet-ide.com.mx reject-with icmp:port-unreachable
joseantoniore@JoseToni: ~$
```

6. Describa que acciones hace ACCEPT, DROP Y RETURN, en IPTABLES

**ACCEPT (Aceptar):** Esta acción le dice al firewall que deje pasar el paquete. Una vez que un paquete coincide con una regla que tiene la acción ACCEPT, el firewall deja de revisar más reglas en esa cadena y permite que el paquete continúe su camino hacia su destino (una aplicación, el sistema operativo, etc).

**DROP (Descartar):** Esta acción le dice al firewall que descarte el paquete silenciosamente. El paquete simplemente se elimina, y no se envía ninguna notificación o mensaje de error al remitente. Desde el punto de vista del remitente, es como si el paquete se hubiera perdido en la red; su conexión simplemente esperará hasta que se agote el tiempo de espera (timeout). Es útil para hacer que tu sistema sea "invisible" a escaneos de red.

**RETURN (Regresar):** Esta acción es un poco más avanzada. Significa "dejar de procesar las reglas en esta cadena y volver a la cadena anterior". Se usa principalmente cuando tienes cadenas personalizadas. Imagina que desde la cadena INPUT "saltas" a una cadena personalizada llamada REGLAS\_WEB. Si un paquete dentro de REGLAS\_WEB coincide con una regla RETURN, dejará de ser evaluado en REGLAS\_WEB y volverá a la cadena INPUT justo en el punto donde se fue, para seguir siendo evaluado por las reglas restantes de INPUT. Si se usa en una cadena principal como INPUT, simplemente aplica la política por defecto de la cadena (por ejemplo, ACCEPT).