

iptables

uso

mantener las conexiones ya establecidas:

```
# iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
```

descartar todos los paquetes entrantes:

```
# iptables -P INPUT DROP
```

permitir ping entrante:

```
# iptables -A INPUT -p icmp --icmp-type 8 -s <origen> -d <servidor> -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT -m comment "aceptación PINGs entrantes"
```

permitir conexiones SSH:

```
# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

permitir conexiones OPENVPN:

```
# iptables -A INPUT -p udp --dport 1194 -j ACCEPT
```

volcar información:

```
# iptables-save > volcado-iptables
```

- <https://help.ubuntu.com/community/IptablesHowTo>

instrucciones básicas:

status

- listado reglas: `$ iptables -L {INPUT|OUTPUT} -n -v --line-numbers`

añadir/insertar

- añadir regla:
 - `$ iptables -A {INPUT|OUTPUT} -p tcp --dport <puerto> -j {DROP|ACCEPT}`
- insertar regla: `$ iptables -I {INPUT|OUTPUT} <linea> -s <IP> -j {DROP|ACCEPT}`
- borrar direcciones de red privadas en interfaz pública (IP Spoofing):
 - `$ iptables -A INPUT -i eth1 -s 192.168.0.0/24 -j DROP`
 - `$ iptables -A INPUT -i eth1 -s 10.0.0.0/24 -j DROP`

eliminar

- borrar regla: `$ iptables -D {INPUT|OUTPUT} <linea>`

- borrar regla (por IP): `$ iptables -D {INPUT|OUTPUT} -s <IP> -j DROP`

save-restore

- guardar reglas: `$ iptables-save > mis.reglas`
- restaurar reglas: `$ iptables-restore < mis.reglas`
- bloquear:
 - IP: `$ iptables -A INPUT -s 1.2.3.4 -j DROP`
 - RED: `$ iptables -A INPUT -s 192.168.1.0/24 -j DROP`
 - PUERTO: `$ iptables -A INPUT -p tcp -dport <puerto> -j DROP`
 - PUERTO+IP: `$ iptables -A INPUT -p tcp -s <ip o red> -dport <puerto> -j DROP`
 - IP (de salida): `$ iptables -A OUTPUT -d <IP o RED> -j DROP`
 - MAC: `$ iptables -A INPUT -m mac --mac-source XX:XX:XX:XX:XX:XX -j DROP`
 - MAC + PUERTO: `$ iptables -A INPUT -p tcp --destination-port 22 -m mac --mac-source 00:0F:EA:91:04:07 -j ACCEPT`
 - PING: `$ iptables -A INPUT -p icmp --icmp-type echo-request -j DROP`
 - PING: `iptables -A INPUT -s 192.168.1.0/24 -p icmp --icmp-type echo-request -j ACCEPT`
 - bloquear dominio:
 - averiguar IP: `$ host -t a www.facebook.com`
 - averiguar el CIDR: `$ whois <IP> | grep CIDR`
 - `$ iptables -A OUTPUT -p tcp -d <CIDR> -j DROP`
 - o también con los nombres de dominio: `$ iptables -A OUTPUT -p tcp -d www.facebook.com -j DROP`
 - añadir comentarios al LOG: `$ iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j LOG --log-prefix «IP SPOOFING A:» * LOG+limites LOG (elimina spoofing cada 5 minutos en ráfagas de 7 entradas): $ iptables → INPUT -i eth1 -s 10.0.0.0/8 -m limit --limit 5/m --limit-burst 7 -j LOG --log-prefix «IP SPOOFING A:»`

/via: <http://elbauldelprogramador.com/20-ejemplos-de-iptables-para-sysadmins/>

opciones

- `$ iptables -L -v` → listar reglas
- `$ iptables -D <chain> <regla>` → borrar regla
- `$ iptables -I <chain> <nº regla>` → insertar * `$ iptables -A <chain> <nº regla>` → insertar

```
$ iptables -A <chain>
-p [tcp|udp]
--dport [mysql]
-j [ACCEPT|REJECT]
-s xxx.xxx.xxx.xxx
-m state
---state NEW,[STABLISHED]
```

From: <https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link: <https://miguelangel.torresegea.es/wiki/linux:tcpip:iptables?rev=1478863365>

Last update: 11/11/2016 03:22



