Filtrado de paquetes
en Linux

Alberto Molina

@alberto_molina

iptables

- Sucesor de ipfwadm e ipchains
- Disponible desde la versión 2.4 del kérnel linux (2001)
- Desarrollado por el proyecto netfilter
- Ampliamente utilizado hoy en día
- Puede trabajar conjuntamente con:
  - ip6tables
  - ebtables
  - arptables
- No se desarrollan ya nuevas funcionalidades

nftables

- Sucesor de {ip,ip6,arp,eb}tables
- Disponible desde la versión 3.13 del kérnel linux (2014)
- Capa de compatibilidad con iptables
- Desarrollado por el proyecto netfilter
- Se otorga más peso al espacio de usuario
- Alto rendimiento

bpfilter

- Permite la utilización de bpf en linux
- Incorporado a linux a partir de la versión 4.18 del kérnel (2018)
- Alto rendimiento
- Poco maduro

¿iptables, nftables o bpfilter?

- iptables está muy establecido y hay reticencia al cambio
- nftables es la evolución natural, es ya una opción totalmente utilizable
- Las dos grandes distros Debian y Red Hat han optado por el uso futuro de nftables
- Ahora mismo bpfilter es una opción solo para kérnels a medida y grandes compañías con equipos especializados y necesidades muy concretas