Una de las cosas buenas que tiene NFTables a partir de la versión 0.9.7 y la versión 5.10 del kernel Linux, es la posibilidad de interactuar con el hook **ingress**. Este hook controla los paquetes según entran a la interfaz de red, **antes de que pasen por la cadena prerouting**. Es decir, antes que los datagramas fragmentados se hayan rearmado nuevamente. Este hook es manejado por la familia inet. No puede ser programado en la familia ip o ip6.

Por todo ello, si tenemos una distro de linux con nftables instalado (como mínimo 0.9.7) y con kernel 5.10 o superior, podemos bloquear los paquetes que entren a la interfaz eth1 y que tengan como destino la subred 192.168.0.0/24, mediante los siguientes comandos de terminal:

Primero creamos la tabla, por si no existe, con:

```
nft add table inet filter
```

Luego creamos la cadena específica para la interfaz eth1, con:

```
nft add chain inet filter ingresseth1 '{ type filter hook ingress device eth1 priority filter; policy accept; }'
```

Y, finalmente, creamos las reglas de bloqueo:

```
nft add rule inet filter ingresseth1 ip daddr 192.168.0.0/24 counter accept
```

Si, a posteriori queremos insertar una regla en una posición anterior a la regla que acabamos de crear, podemos poner, por ejemplo:

```
nft insert rule inet filter ingresseth1 ip daddr 192.168.0.1 counter accept
```

Esta última regla nos permitiría que entraran a la interfaz eth1 paquetes que tengan como destino la IP 192.168.0.1, aún habiendo bloqueado todo el tráfico hacia la subred 0.0/24, dado que esta última regla, al insertarla (y no agregarla) haría match primero.