Estándar

Sólo tienen en cuenta las IPs de la red de origen. No tienen en cuenta protocolos ni puertos.
Se ubican lo más cerca del destino posible.

```
ip access-list standard 1-99 (O nombre)
  deny 192.168.1.0 0.0.0.255
  permit any
exit
int gi2/0
  ip access-group 1-99 (O nombre) out
  exit
```

Extendida

Tienen en cuenta, tanto las IPs de origen, como las de destino. También tienen en cuenta protocolos y puertos.
Se ubican lo más cerca posible al origen.

```
ip access-list extended 100-199 (O nombre)
  deny tcp 192.168.6.0 0.0.0.255 192.160.5.231 0.0.0.255 eq 80
  deny tcp 192.168.6.0 0.0.0.255 192.168.5.231 0.0.0.255 eq 443
  deny udp 192.168.6.0 0.0.0.255 192.168.5.226 0.0.0.255 eq 53
  deny icmp 192.168.6.0 0.0.0.255 192.168.5.224 0.0.0.31
  permit ip any any
  exit
int gi2/0
  ip access-group 100-199 (O nombre) in
  exit
```

Otra forma:

```
ip access-list extended 100-199 (O nombre)
  deny tcp 192.168.6.0 0.0.0.255 192.160.5.231 0.0.0.255 neq 80
  deny tcp 192.168.6.0 0.0.0.255 192.168.5.231 0.0.0.255 gt 443
  permit ip any any
  exit
int gi2/0
  ip access-group 100-199 (O nombre) in
  exit
```

Reflexiva

Permiten controlar que una conexión pueda darse en un sentido, pero no en sentido inverso.
En Packet Tracer sólo puede hacerse con tcp. Ni udp, ni icmp, etc.
Se ubica en la interfaz más cercana al punto de retorno de los paquetes. Es decir, en la primera interfaz que se encuentra el paquete después de empezar a volver.
Se declara como una access-list extendida con el agregado de la palabra established.

Sólo hay que prestar atención a cuales son las IPs de origen. En este caso serían las del punto de retorno.

```
ip access-list extended 100-199 (O nombre)
  permit tcp 192.160.5.231 0.0.0.255 192.168.6.0 0.0.0.255 established
  exit
int gi2/0
  ip access-group 100-199 (O nombre) in
  exit
```

ADVERTENCIA SOBRE REFLEXIVAS: Cuidado con estas reglas reflexivas, porque el origen del tráfico no es la IP de la red permitida, sino la/las IPs de la red bloqueada. Te puedes confundir con esto porque creerás seguramente que el origen es desde donde sale el primer ping, pero no.
NOTA: Para visualizar las listas de acceso que tiene configurada un router, ejecuta como enabled:

```
show access-list
```

ADVERTENCIA: Sólo se puede tener **1 access-group** de entrada y 1 de salida en cada interfaz. Si metes un nuevo access-group de entrada o de salida en una interfaz que ya tenía uno, ¡quitarás de esa interfaz el access-group anterior! Lo mejor, en este caso, sería ir acumulando los deny anteriores en cada nuevo access-list que quieras vincular a esa interfaz.
NOTA: Recuerda no poner ACLs en interfaces loopback, porque las ACLs no filtran paquetes originados desde el mismo router. Es decir, por ejemplo, imagina que el router recibe un ping en la interfaz física. Bien, pues si el router calcula que el ping estaba dirigido a una interfaz que él mismo tiene, no va a reenviar el paquete hacia la interfaz de loopback. Responderá el ping él mismo y no verás matches en las ACLs que pongas en la propia interfaz de loopback. Lo que sí puedes hacer es poner las ACLs, aunque éstas sólo sean de reglas sobre la loopback, en la interfaz física por donde entran osalen los paquetes.