Document Name: ACLs
Access Control Lists or ACLs are used to permit or deny traffic based on the source and or destination IP address. They can be used to identify traffic as well. If you would like to read Cisco's documentation you can do so here.

Standard ACLs

Standard ACLs only look at the source IP address. They are better to user closer to the destination.

1-99 Standard ACL range
1300-1999 Expended standard ACL range

router(config)# access-list [standard ACL number] [permit or deny] A.B.C.D [wild card mask]
router(config)# interface [desire interface to apply ACL]
router(config-if)# ip access-group [ACL number] [in or out]

Extended ACLs

Extended ACLs look at both the source and destination IP address as well as the protocol used. They are better used closer to the source of the traffic.

100-199 Extended ACL range
2000-2699 Expanded Extended ACL range

router(config)# access-list [ACL number] [permit or deny] [ICMP, IP, TCP, or UDP] [Source IP and wildcard mask or any] [Destination IP and wildcard mask or any] [port number]

It is the same process to apply to an interface as it is a standard ACL. To note that the port number on the end is not required.

Editing ACLs and Sequence Numbers

To edit ACLs you have to enter ACL config mode to edit them.

router(config)# ip access-list [extended or standard] [ACL name or number]
router(config-[ext or std]-nacl)#

To delete an ACL rule.

router(config-[ext or std]-nacl)# no [sequence number of ACL]

To add an ACL to an existing list with a custom sequence number.

router(config-[ext or std]-nacl)# [sequence number] [ACL rule, either standard or extended]

Established Keyword

You can use this keyword when using an extended ACL when specifying TCP. This will allow traffic back in that was established by a device from the inside but will not allowing thing else, only established connections. An example is below.

router(config-ext-nacl)# permit tcp any 10.0.1.0 0.0.0.255 established

This will only allow traffic that was established by the 10.0.1.0/24 network.

Show Commands

router# show access-lists
router# show access-lists [ACL name or number]
router# show ip access-lists