1. The lab requires the following security policy to be implemented

|  |  |  |
| --- | --- | --- |
|  | Policy statement | Commands implementing the statement |
| ACL 101 | The only traffic from 192.168.1.0/24 network should be permitted to leave the internal network. | 10 permit ip 192.168.1.0 0.0.0.255 any  20 deny ip any any |
| ACL 102 | Only responses to requests that originated from within the corporate network are allowed back into that network. This includes TCP-based requests from internal hosts such as Web and FTP.  ICMP is allowed into the network fortroubleshooting purposes so that incoming ICMP messages generated in response to pings can be received by internal hosts.  No other network should be able to access the corporate zone. | 10 permit tcp any any established  20 permit icmp any any echo-reply  30 permit icmp any any unreachable  40 deny ip any any |
| ACL 121 | Only HTTP traffic is allowed to the DMZ web server (simulated by Lo0 on HQ)  Other network related traffic, such as EIGRP, is allowed from outside networks  Furthermore, valid internal private addresses, such as 192.168.1.0, loopback address such as 127.0.0.1 and multicast addresses are denied entrance to the corporate network to prevent malicious network attacks from outside users | 10 permit tcp any host 192.168.4.1 eq www  20 deny icmp any host 192.168.4.1  55 deny ip any host 192.168.4.1  60 permit ip any any  30 deny ip 192.168.1.0 0.0.0.255 any  40 deny ip 127.0.0.0 0.255.255.255 any  50 deny ip 224.0.0.0 31.255.255.255 any  70 deny ip any any |

2.Consider the following ACL entry: access-list 102 permit tcp any any established.

How does a firewall distinguish TCP traffic packets that belong to already established connections from any other TCP traffic packets?

There are flags in the TCP header including the ACK. If ACK = 1, then this is a response packet in response to our connection request. Therefore, firewall can distinguish rather it is a TCP traffic packet or not by the ACK flag. If it equals 1 then it is a TCP traffic belonging to established connection. Otherwise, it’s not.