Q. Perform Ping, traceroute command to google.com .

PING:**`ping`** is a utility used to test the connectivity between your machine and a remote host (another computer or server) over a network.

```
C:\Users\290427>ping google.com

Pinging google.com [142.250.183.14] with 32 bytes of data:
Reply from 142.250.183.14: bytes=32 time=50ms TTL=58
Reply from 142.250.183.14: bytes=32 time=157ms TTL=58
Reply from 142.250.183.14: bytes=32 time=57ms TTL=58
Reply from 142.250.183.14: bytes=32 time=52ms TTL=58

Ping statistics for 142.250.183.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 50ms, Maximum = 157ms, Average = 79ms
```

TRACEROUTE: **`traceroute`** (or **`tracert`** on Windows) is a tool that shows the path packets take from your computer to a remote host.

```
C:\Users\290427>tracert google.com

Tracing route to google.com [142.250.67.174]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2    28 ms    27 ms    27 ms  136.226.252.112
  3    30 ms     *        *     136.226.252.2
  4     *       29 ms     *     if-be-25.ecore1.cxr-chennai.as6453.net [180.87.174.41]
  5     *        *        *     Request timed out.
  6    41 ms    40 ms    40 ms  if-ae-3-3.tcore1.cxr-chennai.as6453.net [180.87.36.5]
  7    42 ms     *        *     if-bundle-26-2.qcore1.cxr-chennai.as6453.net [180.87.36.139]
  8    39 ms    37 ms    40 ms  iad23s26-in-f10.1e100.net [173.194.121.42]
  9    43 ms    38 ms    40 ms  216.239.43.137
 10    42 ms    41 ms    40 ms  142.250.208.230
 11    41 ms    41 ms    43 ms  64.233.174.2
 12    64 ms    65 ms    67 ms  142.250.238.206
 13    61 ms    60 ms    58 ms  192.178.110.205
 14    58 ms    59 ms    59 ms  142.250.227.73
 15    65 ms    62 ms    62 ms  bom12s07-in-f14.1e100.net [142.250.67.174]

Trace complete.
```

Q. Design a firewall around a network and open ssh, http and https port on it.

A: To design a firewall around a network and open SSH, HTTP, and HTTPS ports, you would typically follow these steps. The firewall setup will block all incoming traffic by default, except for the specified ports for SSH, HTTP, and HTTPS.

For SSH: Open the port 22 for SSH based traffic.

For HTTP: Open the port 80 for HTTP based traffic.

For HTTPS: Open the port 443 for HTTPS based traffic.