

## 1) Traceroute google.com

The traceroute command can be executed only in linux machines and the windows alternative for traceroute is tracert. The relevant outputs are attached below.

```
Microsoft Windows [Version 10.0.26100.2605]
(c) Microsoft Corporation. All rights reserved.

C:\Users\290398>tracert google.com

Tracing route to google.com [142.250.195.174]
over a maximum of 30 hops:

  0  *          *          *          Request timed out.
  1  29 ms      125 ms     28 ms     136.226.242.122
  2  31 ms      *          *          136.226.242.3
  3  33 ms      30 ms     30 ms     ix-be-26.ecore1.cxr-chennai.as6453.net [180.87.174.45]
  4  57 ms      33 ms     33 ms     209.85.149.232
  5  34 ms      39 ms     30 ms     216.239.43.133
  6  33 ms      38 ms     32 ms     142.251.55.91
  7  34 ms      32 ms     30 ms     maa03s41-in-f14.1e100.net [142.250.195.174]

Trace complete.
```

## Ping google.com

In windows machine the ping command is performed to google.com and relevant outputs are presented below.

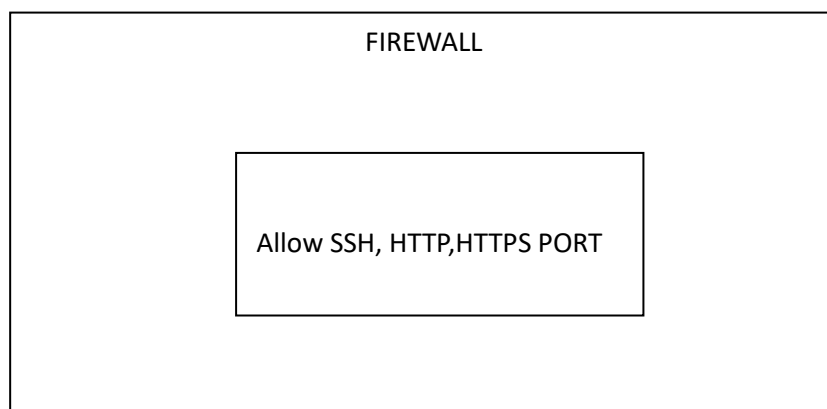
```
C:\Users\290398>ping google.com

Pinging google.com [142.250.183.110] with 32 bytes of data:
Reply from 142.250.183.110: bytes=32 time=55ms TTL=58
Reply from 142.250.183.110: bytes=32 time=63ms TTL=58
Reply from 142.250.183.110: bytes=32 time=58ms TTL=58
Reply from 142.250.183.110: bytes=32 time=61ms TTL=58

Ping statistics for 142.250.183.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 55ms, Maximum = 63ms, Average = 59ms

C:\Users\290398>
```

## 2) Design a network with firewall and open ssh, http and https port.



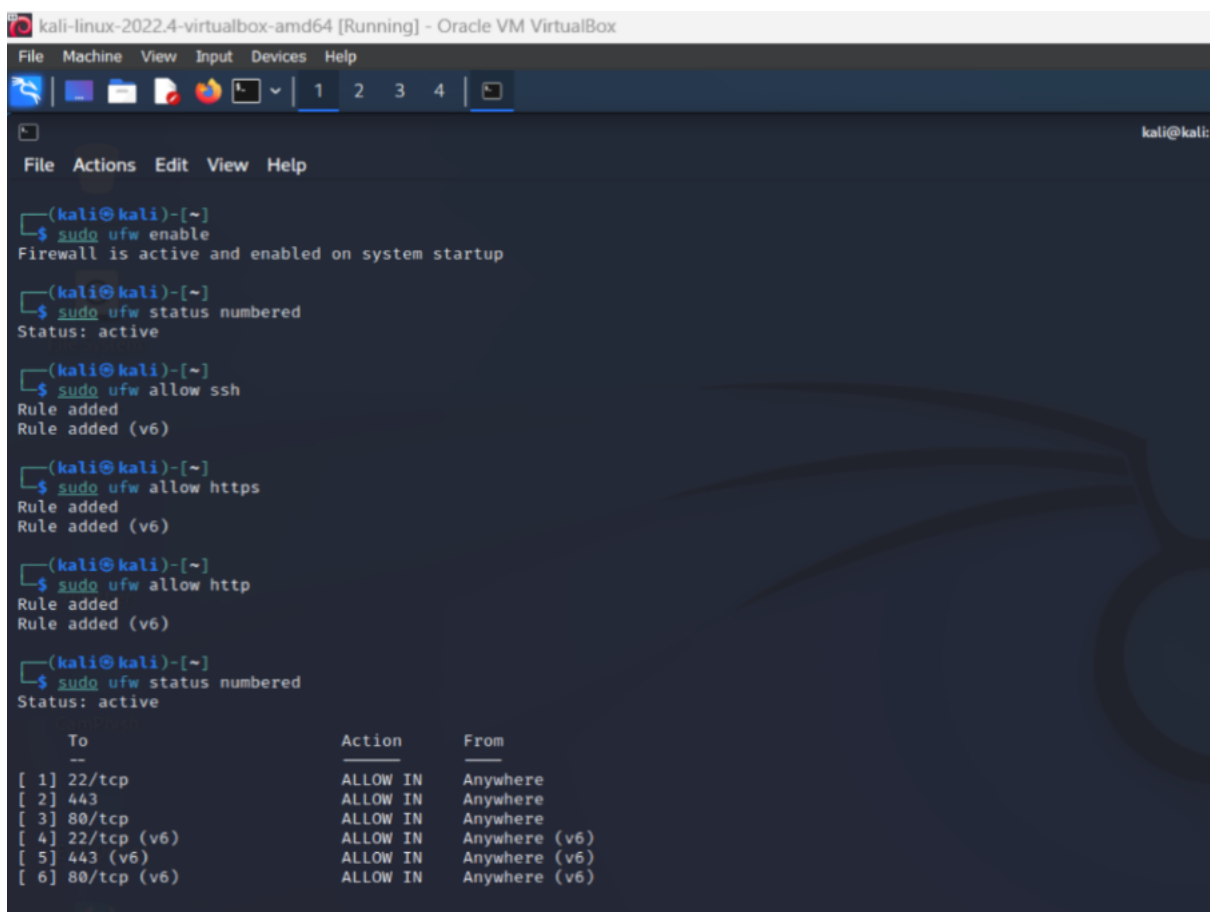
## NETWORK

To design a network with a firewall that allows open SSH (port 22), HTTP (port 80), and HTTPS (port 443), here's how you can structure it:

```
sudo ufw allow ssh
```

```
sudo ufw allow http
```

```
sudo ufw allow https
```



```
kali-linux-2022.4-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4

(kali@kali)-[~]
$ sudo ufw enable
Firewall is active and enabled on system startup

(kali@kali)-[~]
$ sudo ufw status numbered
Status: active

(kali@kali)-[~]
$ sudo ufw allow ssh
Rule added
Rule added (v6)

(kali@kali)-[~]
$ sudo ufw allow https
Rule added
Rule added (v6)

(kali@kali)-[~]
$ sudo ufw allow http
Rule added
Rule added (v6)

(kali@kali)-[~]
$ sudo ufw status numbered
Status: active

      To Action From
      --
[ 1] 22/tcp ALLOW IN Anywhere
[ 2] 443 ALLOW IN Anywhere
[ 3] 80/tcp ALLOW IN Anywhere
[ 4] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 5] 443 (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
```