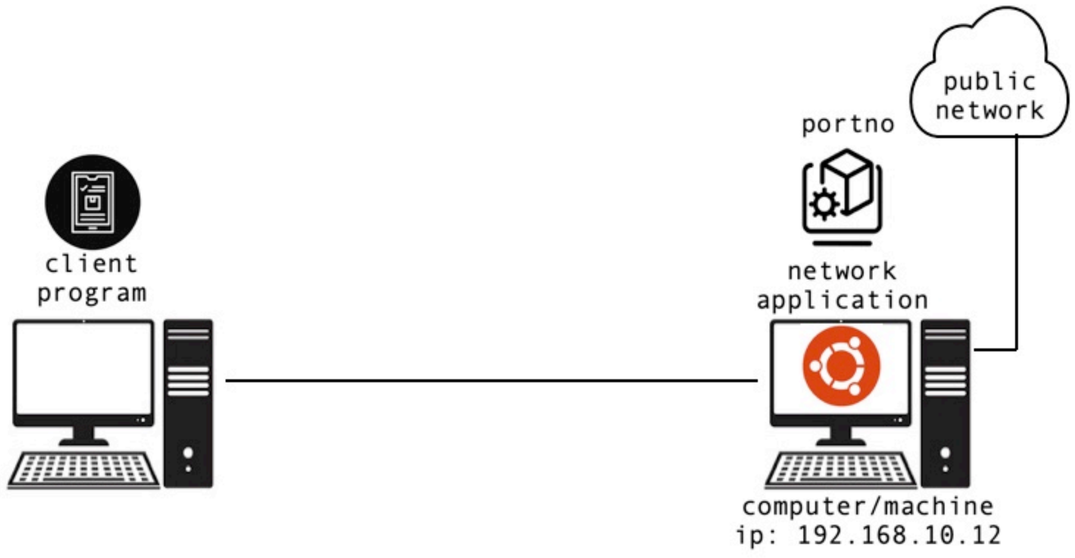

Network application:
allows the user to access the program over the network using application protocols
1. http
2. smtp
3. ftp
4. imap
5. pop3
6. jrmp
7. iiop
etc

Server program: must and should have a portno that acts as logic address or identity of the program within the computer.

A server program opens up a portno allowing the client applications to connect and communiate withit over the network. If any program opens a portno on a computer, it opens a door to the world, which means anyone can connect and communicate with that program, thus posing a security risk.

While browsing or surfing the internet, un-knowingly they can be malicious programs/software could download on our computer and opens a port letting the hacker to connect and steal the data on our computer. The general user of the computer may not be aware of the information such information and might be prone to security threat or risk of lossing the data.

How to prevent such attacks that happens to the computers that are connected to the network?
The operating system should be able to provide a sophisticated / secured environment letting the users to use the computer, so most of the operating system provides an software called “Firewall” through which we can monitor, manage, grant, deny permissions to the programs opening ports and communicate over the network.

Firewall is an network security software provided by most of the operating system in control of incoming/outgoing network traffic from the computer. The users of the computer can configure firewalls defining allowing the programs to
 1. which ports are allowed/denied
 2. which protocol requests allowed/denied
 3. what ip addresses from where the requested/responses are allowed/denied

There are 2 types of firewalls are there
1. firewall as an software that is installed within the operating system of the computer
2. hardware firewalls that sits at network level, to manage, monitor and restrict network traffic for the group of computers over the network.