What is purpose of the server?
- The server program runs on a port number will allow the web pages / static web site to be accessible across the network using HTTP protocol. Now the people/client systems across the network can send http protocol requests in accessing the web pages using ip:portno with web pages so that server program receives the request and dispatches the web pages to the client

There are lot of HTTP protocol supported server programs are availabe freely one of such popular Http Server program is apache2.

apache2 http server allows us to host multiple static websites on a single host computer through virtual host configuration.

1. Install apache2

```
sudo apt update
sudo apt install -y apache2
```

2. where does apache2 server installed

```
/etc/apache2
|-sites-available
|-sites-enabled
|-conf
```

3. create static websites under /var/www

```
/var/www
|-localnews
|-public_html
|-*.html
|-regionalnews
|-public_html
|-*.html
```

4. chown to change group/user of the static website directories
5. chmod 755 to files/folders of static website

6. create virtual host configuration files

```
/etc/apache2/sites-available
|-localnews.conf
|-regionalnews.conf
```

localnews.conf

```
<VirtualHost *:80>
ServerName localnews
DocumentRoot /var/www/localnews/public_html
</VirtualHost>
```

regionalnews.conf

```
<VirtualHost *:80>
ServerName regionalnews
DocumentRoot /var/www/regionalnews/public_html
</VirtualHost>
```

7. enable apache2 site

```
sudo a2ensite siteName
```

8.sudo systemctl reload apache2

Firewall = is a hardware device sits on a computer network (or) could be a software program install on a computer device to monitor and control the network traffic to a computer (or) network of computers.

We can configure rules in the Firewall allowing/denying the network traffic based on
1. port
2. ip address
3. protocol

-> block all the http protocol requests to my computer
-> block network traffic from an specific ip address computer to my computer
-> block port: 9099 on my computer
by using these we can secure the network traffic towards our computer.
----
ubuntu operation system comes with firweall called "iptables", iptables is touch to configure and is not easy for general user to manage firewall.
so to ease the use of iptables ubuntu has provided an interface "ufw" its a software through which we configure iptables of ubuntu.

ufw = "Uncomplicated Firewall" = ufw software package through which we configure iptables of ubuntu to enforce restrictions on network traffic.

Firewall = it is a software application or a hardware device used for monitoring and controlling the network traffic on a computer or on a network of computers.

A computer can be accessed by any other computers over the network if those are inter-connected,but we want to impose traffic restrictions on what can the other computers can access from my computer by using firewall.
The restrictions could be like
1. the ip address of the machine who can allowed to access/denied to access
2. the programs running on a port who can access those programs
3. type of the protocol used to access the programs of my computer.

Ubuntu distribution comes up with iptables as the default firewall as part of it. iptables are much complex to configure and use it for a general purpose user, it requires knowledge on iptables and networking and protocols etc.
to manage in easily configuring iptables, ubuntu has provided a software package called "ufw" stands for Un-Complicated Firewall.

#1
ufw comes with default installation from Ubuntu-18.0
in case if you want to install you can gothrough package manager

```
sudo apt install -y ufw
```

#2 by default ufw setup the traffic rules/policies as
deny all the incomming traffic
allow all the outgoing traffic

```
sudo ufw default deny incoming
sudo ufw default allow outgoing
```

#3 by default ufw is installed but disabled. if you want to enable ufw
sudo ufw enable = ufw will be enabled now

```
sudo ufw disable
```

#4 if we to see the existing routing policies of ufw

```
sudo ufw status verbose
```

#5 we can allow or deny traffic based on protocol

```
sudo ufw allow protocol
```

#6 we can delete ufw traffic policies/rules based on numbers

```
sudo ufw status numbered
```

it displays all the rules with numbers then run

```
sudo ufw delete ruleNumber
```

#6 allow traffic from source ip address computer of any type of traffic

```
sudo ufw allow from 192.168.1.10
```

#7 allow traffic from source ip address of computer to a specific port.

```
sudo ufw allow from 192.168.1.10 to any port 80
```

----

ssh = secure shell