Firewall Commands-Start

- Launch 2 EC2 instances(EC2-A and EC2-B) with Amazon Linux AMI and allow private ip connection on both in AWS Security Group.
- On EC2-A
- Install httpd, start httpd, write some content to /var/www/html/index.html
- On EC2-B
- Test the request of httpd to the EC2-A instance

```
curl EC2-A-private-ip
```

- The output will be content of the /var/www/html/index.html
- On EC2-A
- install firewalld

```
yum install -y firewalld
```

- Enable the service at boot time

```
systemctl enable firewalld
```

- Start the service

```
systemctl start firewalld

firewall-cmd --state
```

- After the firewalld service is started, test the curl from EC2-B to EC2-A again

```
curl EC2-A-private-ip
```

> By default, firewalld will be active and will reject all incoming traffic with a couple of exceptions, like SSH.

- List information for all zones

```
firewall-cmd --list-all-zones
```

- To check which is the default zone

```
firewall-cmd --get-default-zone

firewall-cmd --list-services
```

- To Enable all the incoming ports for a service

```
firewall-cmd --zone=public --add-service=http

firewall-cmd --list-services
```

- test the curl from EC2-B to EC2-A again

#To List the services that are allowed for the public zone firewall-cmd --zone=public --list-services

#Here only runtime configuration is updated, it is lost if firewalld service is restarted.

```
systemctl restart firewalld
firewall-cmd --zone=public --list-services
```

- Use below command to make this changes permanent

```
firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --zone=public --list-services
```

- Remove a service from a zone

```
firewall-cmd --permanent --zone=public --remove-service=http
```

- Test the curl from EC2-B to EC2-A again
- Traffic can be allowed on specific port

```
firewall-cmd --add-port=[YOUR PORT]/tcp
```

```
firewall-cmd --add-port=80/tcp
```

- To add above permanently

> firewall-cmd --permanent --add-port=[YOUR PORT]/tcp

```
firewall-cmd --permanent --add-port=80/tcp
```

- test the curl from EC2-B to EC2-A again
- To list what ports are open use below

```
firewall-cmd --list-ports
```