Network Security and Firewall Configuration

- Firewall Configuration

Firewall Configuration

Installing and configuring UFW (Uncomplicated Firewall)

Add sudo in front of the commands if you are using a normal account with sudo privileges

Installing UFW

1. Use the command below to ensure that UFW is installed

```
apt-get install ufw
```

Setting up default policies

1. Use the commands the below to set/reset the firewall policies to default

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

These commands set the defaults to deny incoming and allow outgoing connections

Allowing SSH connections

1. Allow SSH connections with the following command

```
ufw allow ssh
```

Enabling UFW

1. To enable UFW, use this command

```
ufw enable
```

You will receive a warning that says the command may disrupt existing SSH connections. We already set up a firewall rule that allows SSH connections, so it should be fine to continue.Respond to the prompt with y

Allowing other connections (examples)

Specific services

```
ufw allow http
```

Specific ports

```
ufw allow 80
```

Port ranges

```
ufw allow 6000:6007/tcp
ufw allow 6000:6007/udp
```

Denying connections

```
Denying services
================

ufw deny http

Denying a port
============

ufw deny 80
```

Checking UFW Status and Rules

```
ufw status verbose
```

The output should look similar to

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

```
To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
```