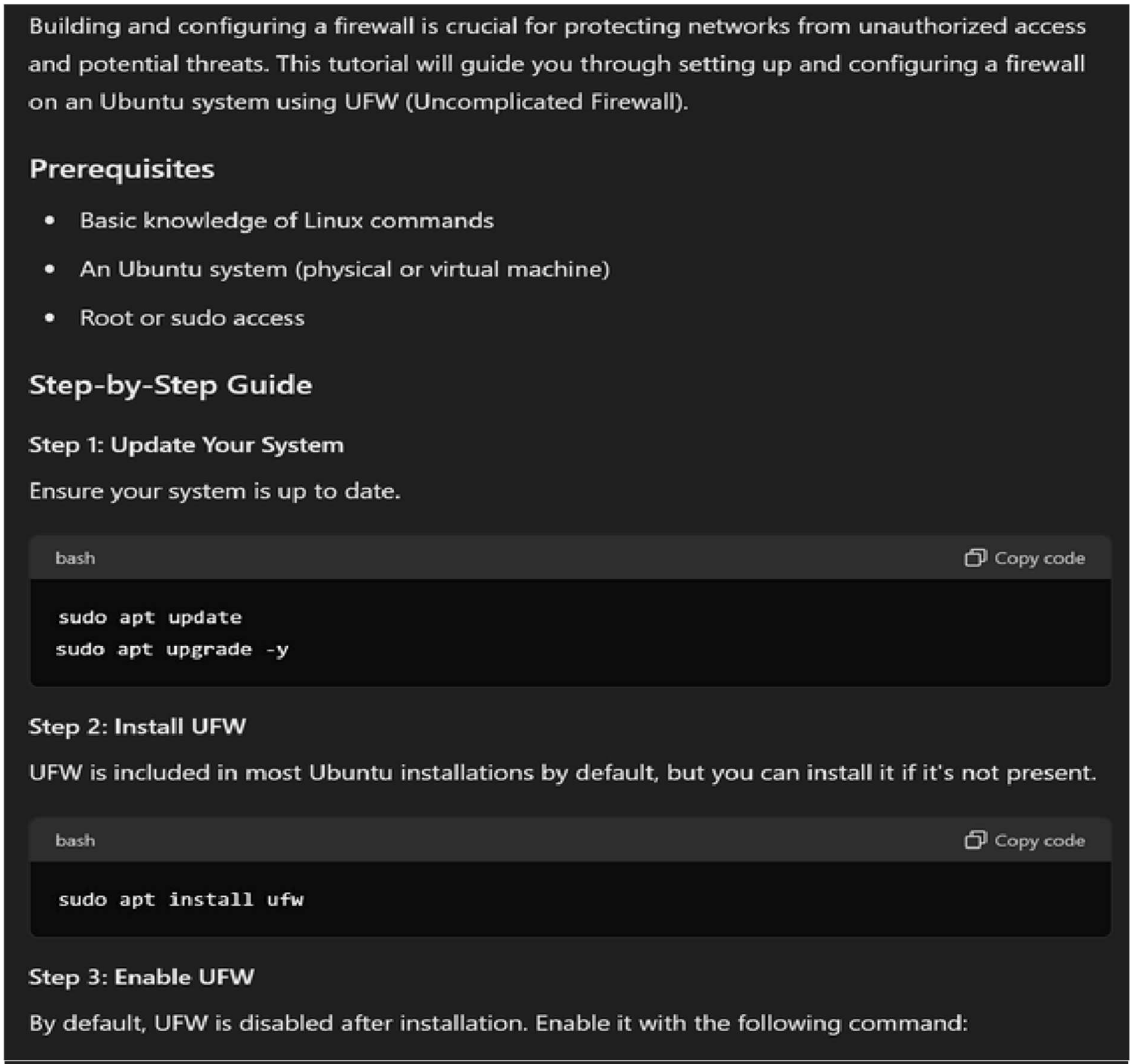
Build and Configure a Firewall



Building and configuring a firewall is crucial for protecting networks from unauthorized access and potential threats. This tutorial will guide you through setting up and configuring a firewall on an Ubuntu system using UFW (Uncomplicated Firewall).

Prerequisites

- Basic knowledge of Linux commands
- An Ubuntu system (physical or virtual machine)
- Root or sudo access

Step-by-Step Guide

Step 1: Update Your System

Ensure your system is up to date.

```bash
sudo apt update
sudo apt upgrade -y
```

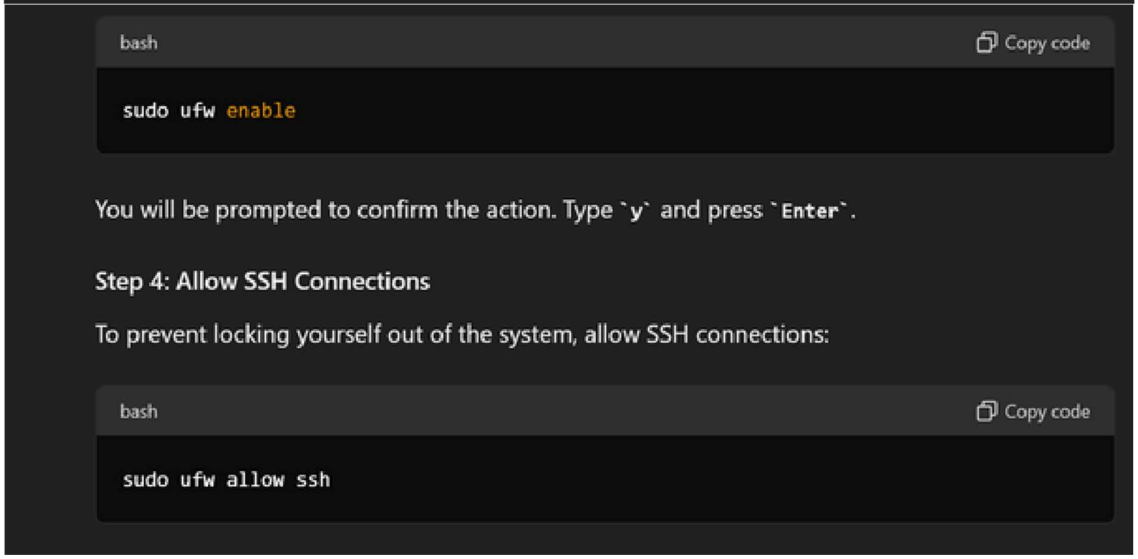
Step 2: Install UFW

UFW is included in most Ubuntu installations by default, but you can install it if it's not present.

```bash
sudo apt install ufw
```

Step 3: Enable UFW

By default, UFW is disabled after installation. Enable it with the following command:



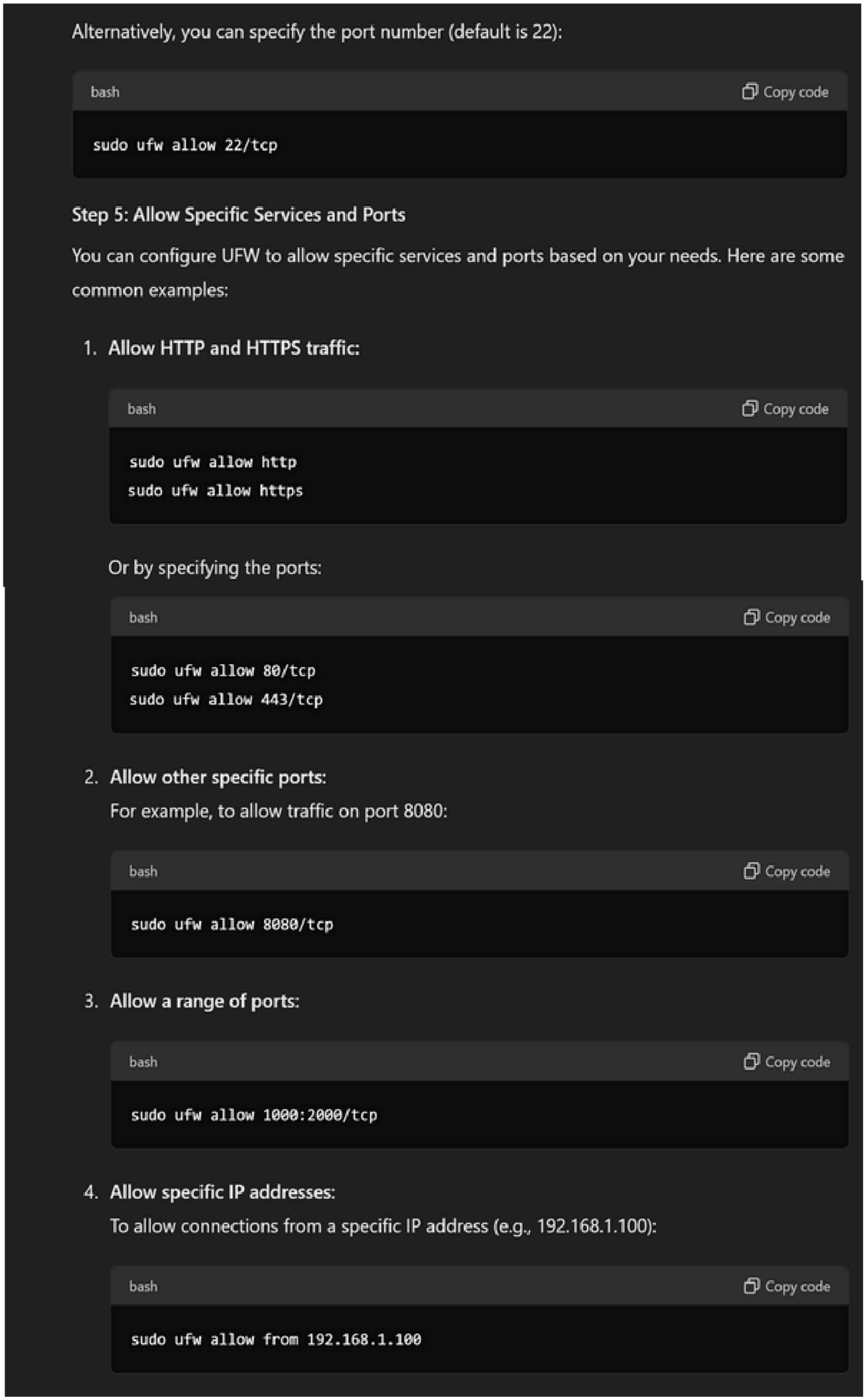
```bash
sudo ufw enable
```

You will be prompted to confirm the action. Type `y` and press `Enter`.

Step 4: Allow SSH Connections

To prevent locking yourself out of the system, allow SSH connections:

```bash
sudo ufw allow ssh
```



Alternatively, you can specify the port number (default is 22):

```bash
sudo ufw allow 22/tcp
```

Step 5: Allow Specific Services and Ports

You can configure UFW to allow specific services and ports based on your needs. Here are some common examples:

1. **Allow HTTP and HTTPS traffic:**

   ```bash
   sudo ufw allow http
   sudo ufw allow https
   ```

   Or by specifying the ports:

   ```bash
   sudo ufw allow 80/tcp
   sudo ufw allow 443/tcp
   ```

2. **Allow other specific ports:**
   For example, to allow traffic on port 8080:

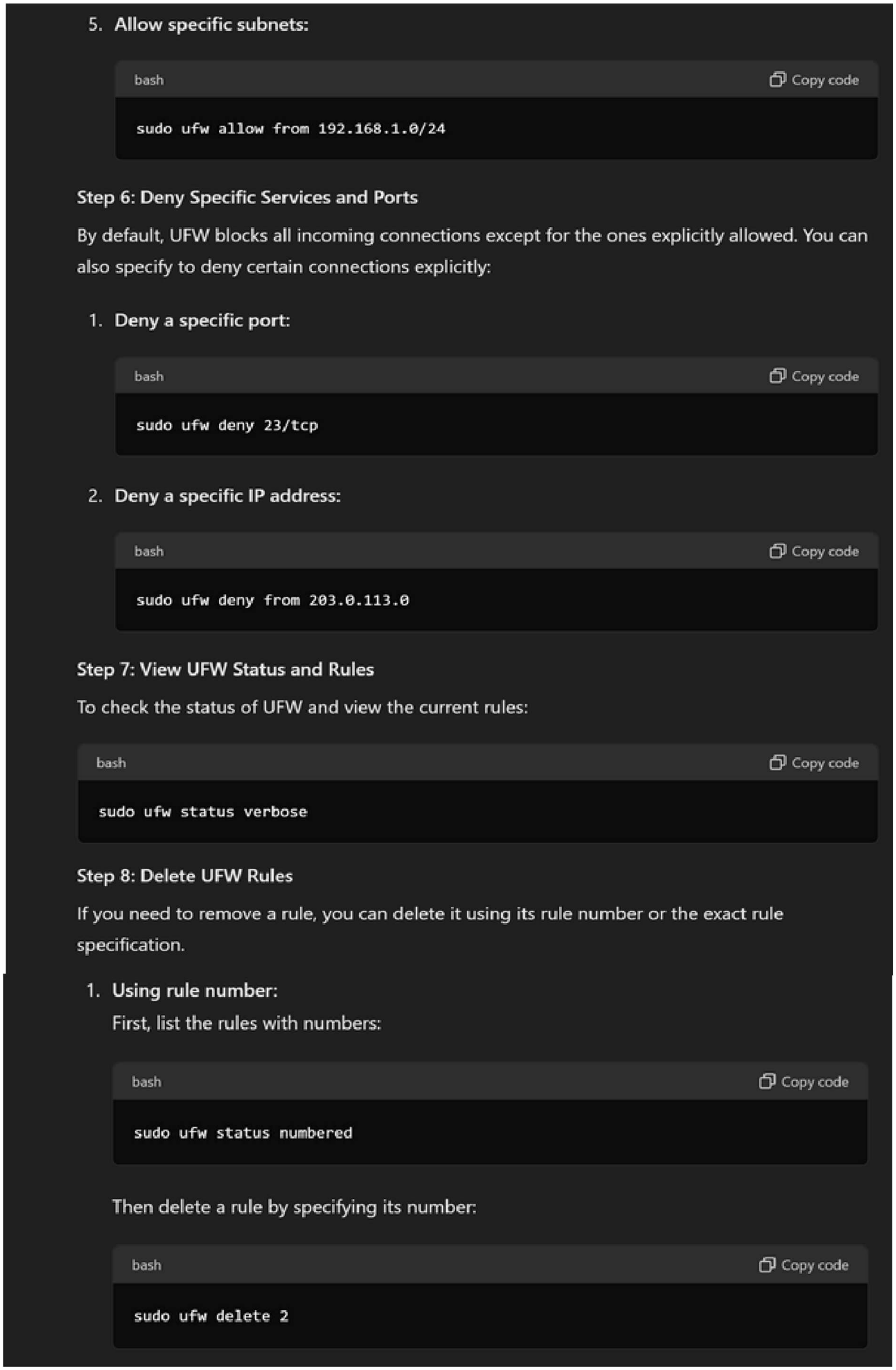
   ```bash
   sudo ufw allow 8080/tcp
   ```

3. **Allow a range of ports:**

   ```bash
   sudo ufw allow 1000:2000/tcp
   ```

4. **Allow specific IP addresses:**
   To allow connections from a specific IP address (e.g., 192.168.1.100):

   ```bash
   sudo ufw allow from 192.168.1.100
   ```



5. **Allow specific subnets:**

```bash
sudo ufw allow from 192.168.1.0/24
```

Step 6: Deny Specific Services and Ports

By default, UFW blocks all incoming connections except for the ones explicitly allowed. You can also specify to deny certain connections explicitly:

1. **Deny a specific port:**

```bash
sudo ufw deny 23/tcp
```

2. **Deny a specific IP address:**

```bash
sudo ufw deny from 203.0.113.0
```

Step 7: View UFW Status and Rules

To check the status of UFW and view the current rules:

```bash
sudo ufw status verbose
```

Step 8: Delete UFW Rules

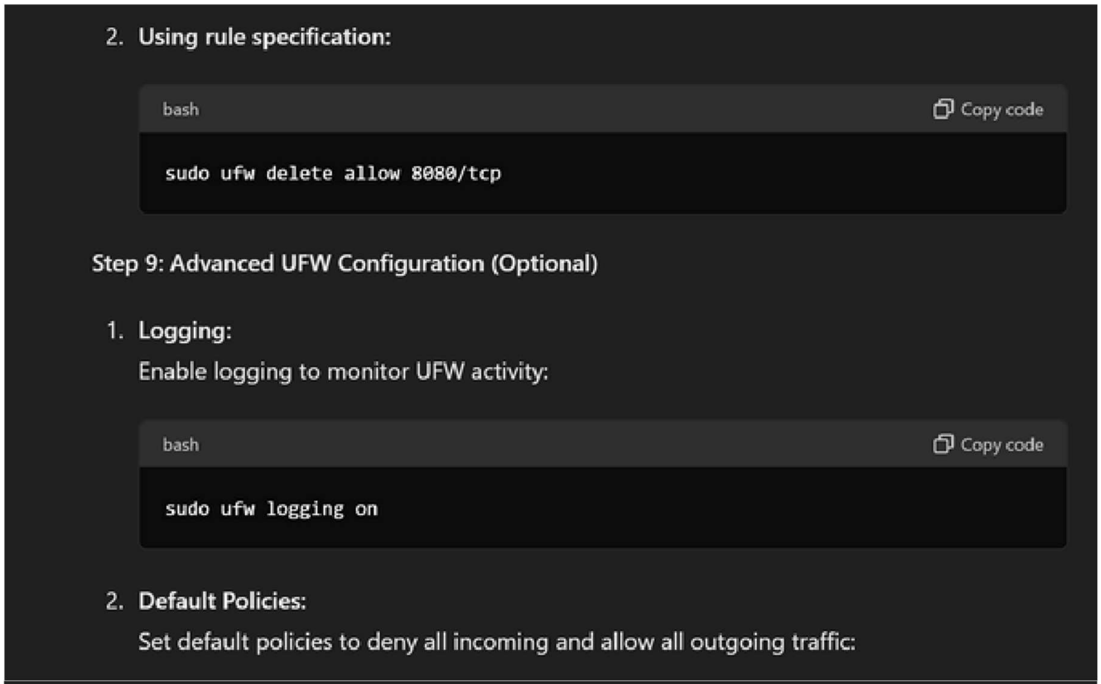
If you need to remove a rule, you can delete it using its rule number or the exact rule specification.

1. **Using rule number:**
   First, list the rules with numbers:

```bash
sudo ufw status numbered
```

Then delete a rule by specifying its number:

```bash
sudo ufw delete 2
```



2. **Using rule specification:**

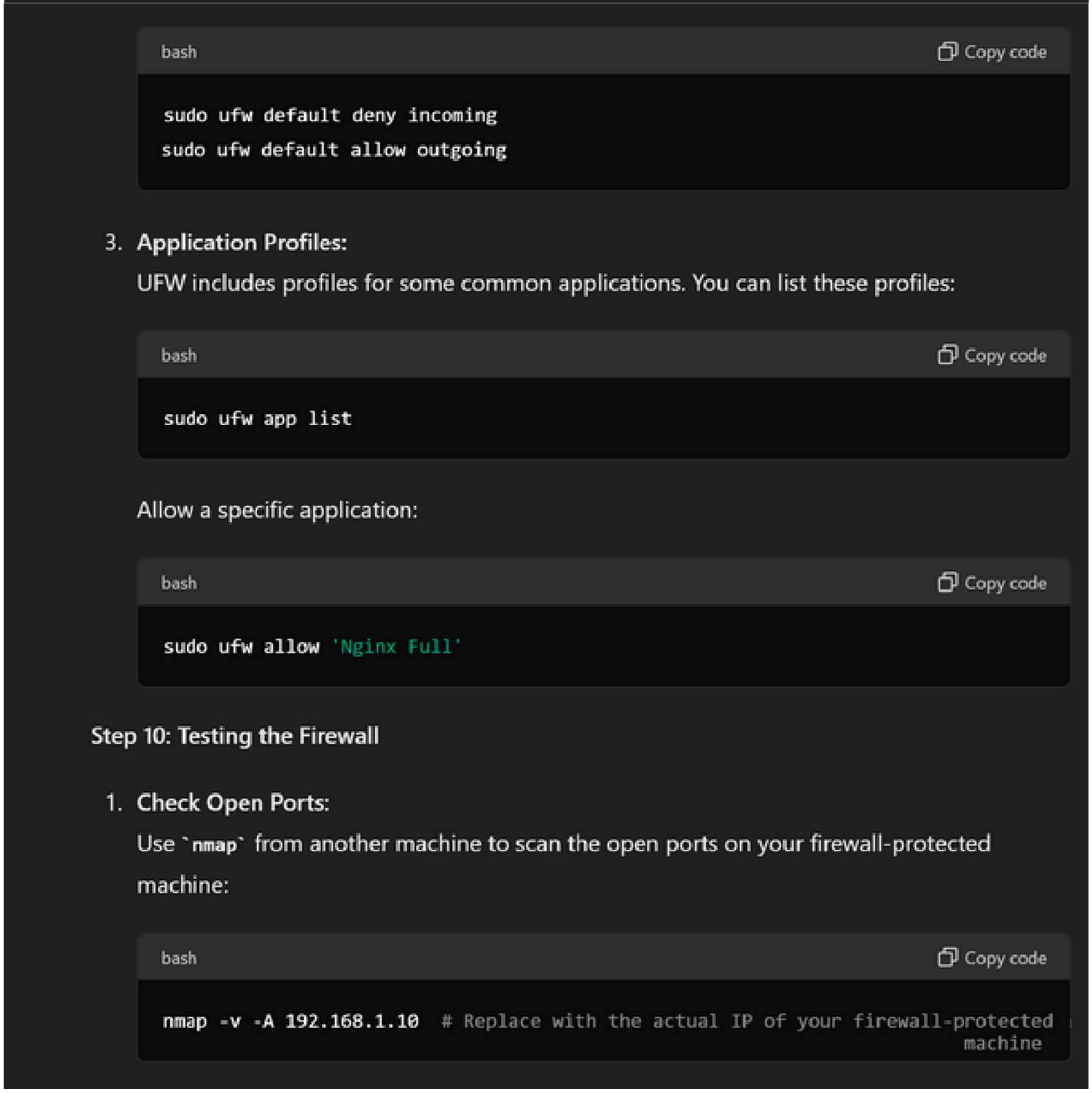
```bash
sudo ufw delete allow 8080/tcp
```

Step 9: Advanced UFW Configuration (Optional)

1. **Logging:**
   Enable logging to monitor UFW activity:

```bash
sudo ufw logging on
```

2. **Default Policies:**
   Set default policies to deny all incoming and allow all outgoing traffic:



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

3. **Application Profiles:**
   UFW includes profiles for some common applications. You can list these profiles:

```bash
sudo ufw app list
```

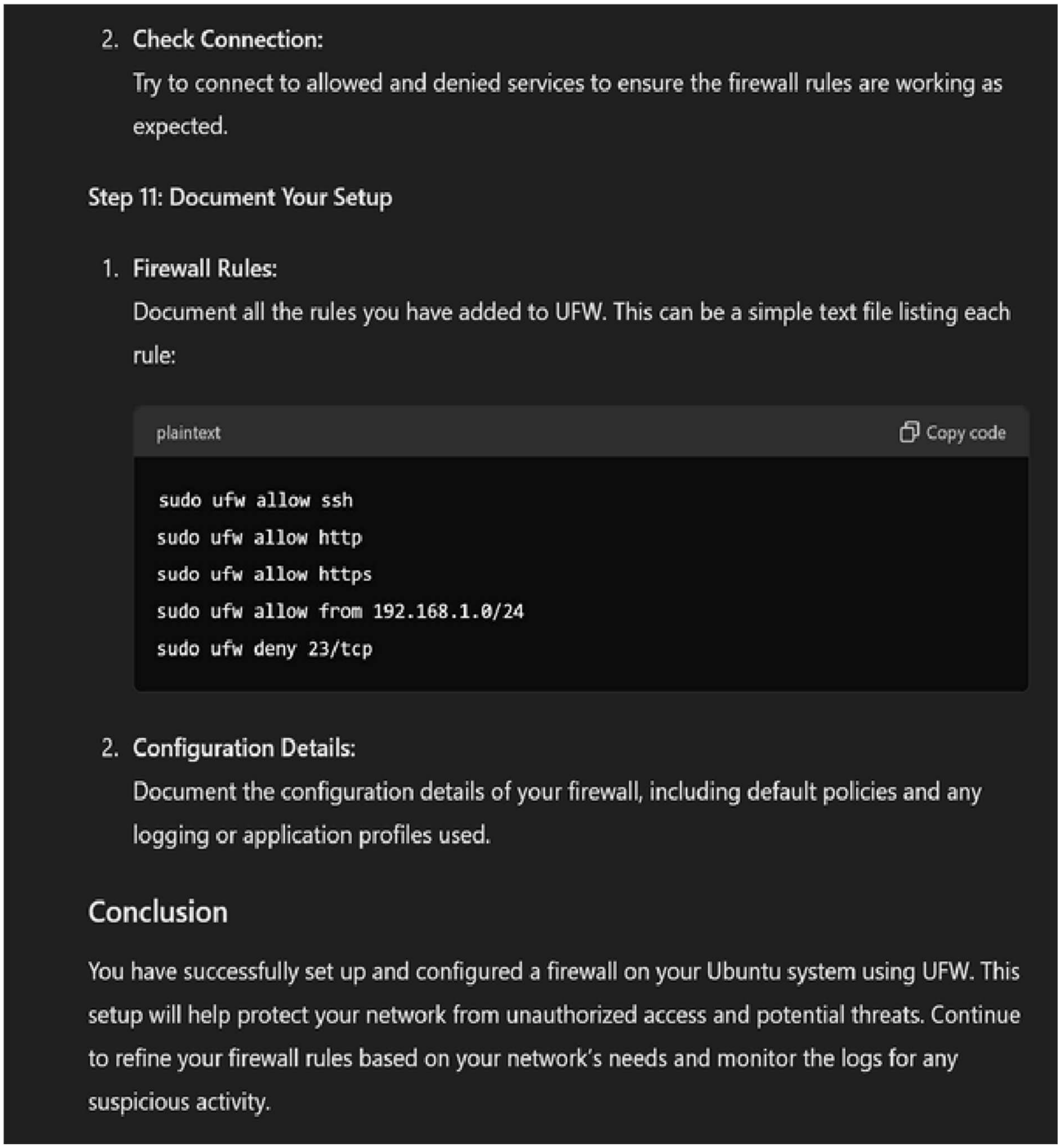
   Allow a specific application:

```bash
sudo ufw allow 'Nginx Full'
```

Step 10: Testing the Firewall

1. **Check Open Ports:**
   Use `nmap` from another machine to scan the open ports on your firewall-protected machine:

```bash
nmap -v -A 192.168.1.10  # Replace with the actual IP of your firewall-protected
                                                                          machine
```



2. **Check Connection:**
   Try to connect to allowed and denied services to ensure the firewall rules are working as expected.

Step 11: Document Your Setup

1. **Firewall Rules:**
   Document all the rules you have added to UFW. This can be a simple text file listing each rule:

```
sudo ufw allow ssh
sudo ufw allow http
sudo ufw allow https
sudo ufw allow from 192.168.1.0/24
sudo ufw deny 23/tcp
```

2. **Configuration Details:**
   Document the configuration details of your firewall, including default policies and any logging or application profiles used.

Conclusion

You have successfully set up and configured a firewall on your Ubuntu system using UFW. This setup will help protect your network from unauthorized access and potential threats. Continue to refine your firewall rules based on your network's needs and monitor the logs for any suspicious activity.

Thanking You