I'll break down the commands you provided and highlight key points:

1. Installing and Enabling UFW:

- **`sudo apt install ufw`:** This installs the Uncomplicated Firewall (UFW), a user-friendly firewall management tool for Ubuntu.
- **sudo ufw default allow outgoing:** This sets the default policy for outgoing traffic to "allow," permitting any outgoing connections.
- **sudo ufw default deny incoming:** This sets the default policy for incoming traffic to "deny," blocking all incoming connections unless explicitly allowed.
- **sudo ufw enable:** This activates UFW and enforces the configured firewall rules.

2. Allowing Specific Ports:

- **sudo ufw allow 80:** This opens port 80 for incoming HTTP traffic, typically used for web servers.
- **sudo ufw allow 443:** This opens port 443 for incoming HTTPS traffic, the secure version of HTTP.
- **sudo ufw allow 53:** This opens port 53 for incoming DNS traffic, used for domain name resolution.
- **sudo ufw allow 3000:** This opens port 3000, which you've chosen for SSH access. However, note that this command alone doesn't change the SSH daemon's listening port. You'll need to follow additional steps to configure SSH to use port 3000.

Additional Steps for Changing SSH Port:

1. **Edit the SSH configuration file:**

   ```
   sudo nano /etc/ssh/sshd_config
   ```

2. **Locate the Port directive:**
   ```
   #Port 22
   ```

3. **Change the port number to 3000:**
   ```
   Port 3000
   ```

4. **Save the file and exit the editor:** (Press Ctrl+O, then Enter, then Ctrl+X)
5. **Restart the SSH service:**

   ```
   sudo systemctl restart ssh
   ```

Important Considerations:

- **Remote Access:** If you're using SSH remotely, make sure to update your SSH client to connect to port 3000 instead of the default port 22.
- **Firewall Configuration:** If you have additional firewalls in place, ensure they also allow traffic on port 3000 for SSH.
- **Security Best Practices:** Regularly review and update your firewall rules to maintain a secure environment.

```
sudo apt install ufw

sudo ufw default allow outgoing

sudo ufw default deny incoming

sudo ufw enable

sudo ufw allow 80

sudo ufw allow 443

sudo ufw allow 53

sudo ufw allow 3000
```