Firewall Installation and Configuration Report

**1. Introduction:**

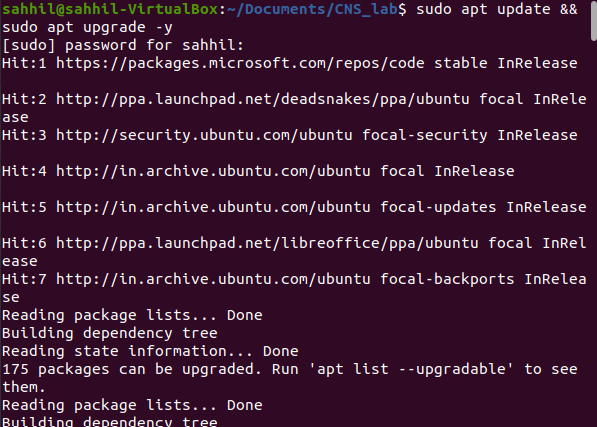
This report outlines the installation and configuration of a firewall using UFW on a Linux system. The firewall has been configured according to the security policy defined for the system, which ensures that only necessary services are exposed, and all other traffic is blocked.

**2. System Overview:**

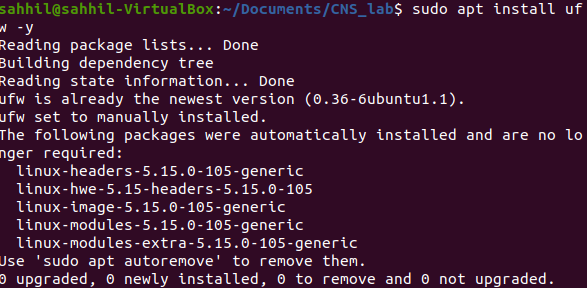
* **Operating System**: Ubuntu 20.04 LTS
* **Firewall Tool**: UFW (Uncomplicated Firewall)
* **Security Policy**:
  + Deny all incoming traffic by default.
  + Allow traffic only for essential services (SSH, HTTP, HTTPS).
  + Log all firewall events for audit purposes.

**3. Firewall Installation Steps:**

1. Updated the system using sudo apt update && sudo apt upgrade.



1. Installed UFW using the command sudo apt install ufw.

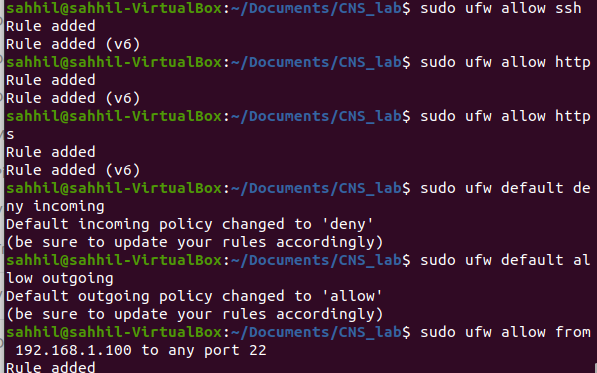


1. Enabled UFW using sudo ufw enable.



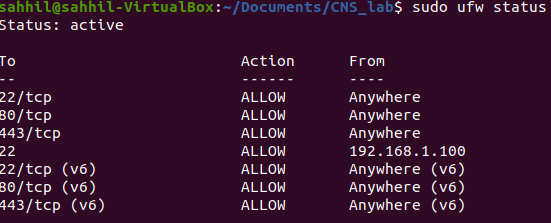
**4. Security Policy Configuration:**

* Allowed SSH (port 22) for remote administration.
* Allowed HTTP (port 80) and HTTPS (port 443) to enable web server access.
* Blocked all incoming traffic by default except for essential services
* Allowed SSH access from a specific IP for added security



5. Current Status and Rules:

The current UFW status shows that the firewall is active with the following rules:



6. Logging:

Firewall logging has been enabled using:



**7. Reload and Apply Changes**

Make sure the firewall is properly reloaded to apply all changes:

