Build and Configure a Firewall

Created by Hasan Williams

This document outlines my process of setting up an Ubuntu virtual machine using VirtualBox, configuring UFW (Uncomplicated Firewall), and verifying server connectivity. It details the technologies I used and what I learned throughout the process.

I've set up a virtual machine named "Ubuntu - Firewall (UFW)" using the Ubuntu24.10 ISO image, configured as Linux (64-bit), and stored it in a designated folder. I allocated 4096 MB of RAM and assigned1 CPU, creating a20 GB virtual hard disk in VDI format. After starting the VM, I successfully installed Ubuntu24.10. For firewall configuration, I updated and upgraded the system, installed UFW, and enabled it. I set up firewall rules to allow SSH, HTTP, HTTPS, and specific ports while denying Telnet. I configured default policies to deny all incoming and allow outgoing connections, managed application and IP permissions, and verified open ports using nmap. To ensure server accessibility, I retrieved the web page using curl, established an SSH connection, verified host authenticity, and confirmed secure access. Finally, I verified HTTPS communication with a successful200 OK status.

Virtual Machine Setup

1. Name and Operating System:
    - I named the VM "Ubuntu - Firewall (UFW)".
    - Stored it in a designated folder.
    - Used the Ubuntu24.10 ISO image.
    - Configured it as Linux, Ubuntu (64-bit).
2. Hardware Configuration:
    - Allocated 4096 MB RAM.
    - Assigned1 CPU.
3. Hard Disk Setup:
    - Created a new virtual hard disk.
    - Set the size to20 GB.
    - Chose the VDI format.
4. Installation and Setup:
    - Started the VM and installed Ubuntu24.10.
    - Successfully reached the Ubuntu welcome screen.

UFW Configuration

1. Update and Upgrade:
    - I ran *sudo apt update* and *sudo apt upgrade -y*.
2. Install and Enable UFW:
    - Installed UFW using *sudo apt install ufw*.
    - Enabled it with *sudo ufw enable*.
3. Firewall Rules:
    - Allowed SSH: *sudo ufw allow 22/tcp*
    - Allowed HTTP/HTTPS: *sudo ufw allow http*, *sudo ufw allow https*

    - Allowed specific ports: *sudo ufw allow 8080/tcp*, *sudo ufw allow1000:2000/tcp*
    - Denied Telnet: *sudo ufw deny 23/tcp*
4. Default Policies:
    - Denied all incoming: *sudo ufw default deny incoming*
    - Allowed all outgoing: *sudo ufw default allow outgoing*
5. Application and IP Management:
    - Allowed Wsdd: *sudo ufw allow 'Wsdd'*
    - Managed IPs: Allowed 192.168.1.100, 192.168.1.0/24; Denied 203.0.113.0
6. Verification:
    - Used nmap to verify open ports.

Server Configuration and Access

1. Web Page Retrieval:
    - I used curl http://10.0.2.15 to confirm Apache2 server accessibility.
2. SSH Connection Setup:
    - Command: ssh hasan@10.0.2.15
    - Verified host authenticity and added it to known hosts.
3. Successful SSH Login:
    - Logged into the server, confirming secure access.
4. HTTPS Response Verification:
    - Command: curl -Ik https://10.0.2.15
    - Confirmed successful HTTPS communication with a 200 OK status.

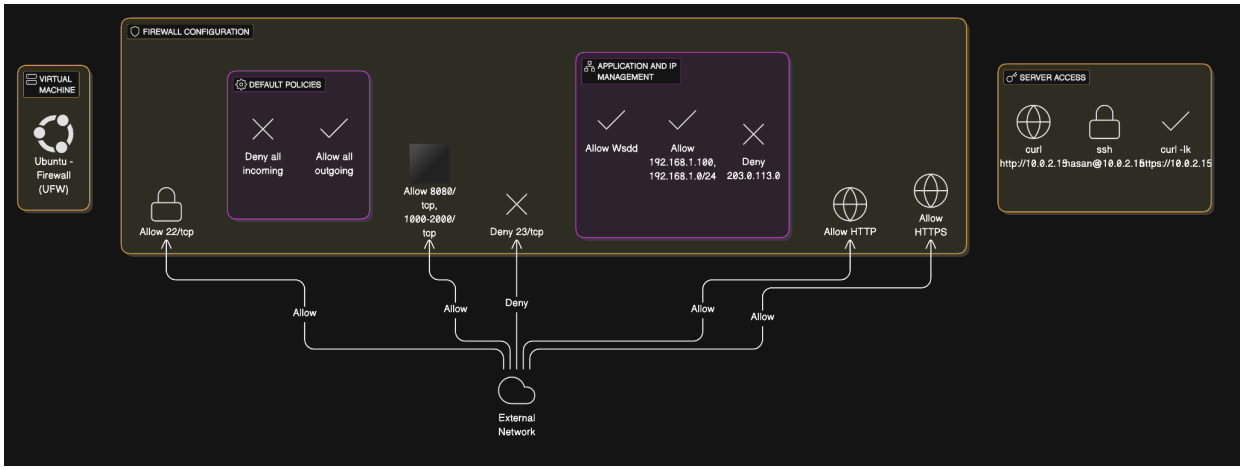
Technologies Used

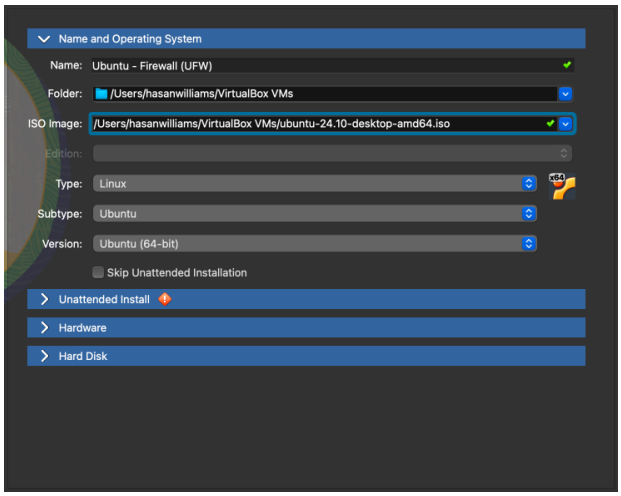
- VirtualBox for virtual machine management.
- Ubuntu 24.10 as the operating system.
- UFW for firewall configuration.
- Curl and SSH for server access and verification.
- Nmap for network scanning.

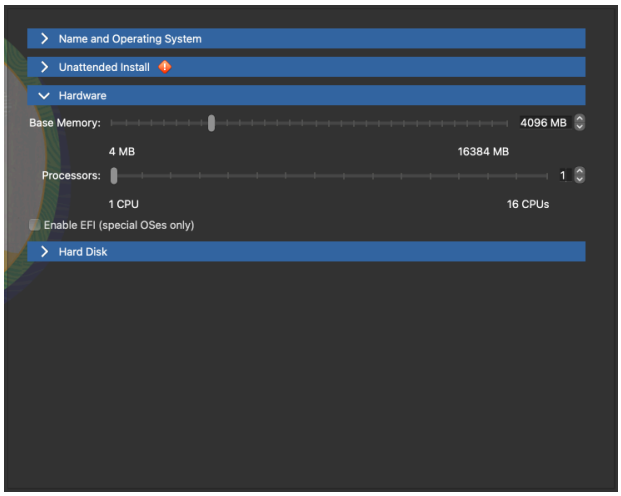
Lessons Learned

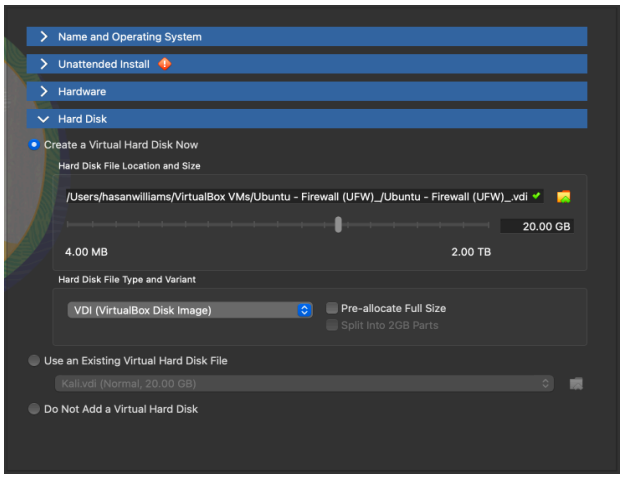
- Virtual Machine Setup: I gained experience in configuring VMs and understanding hardware requirements.
- Firewall Management: I learned to effectively use UFW for managing network traffic and securing the server.
- Server Access: I developed skills in using SSH and curl for remote server management and verification.

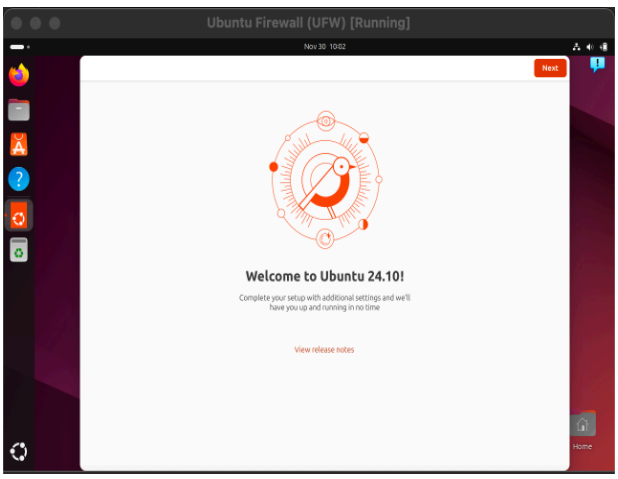
This comprehensive setup and configuration process provided me with valuable insights into system administration and network security.

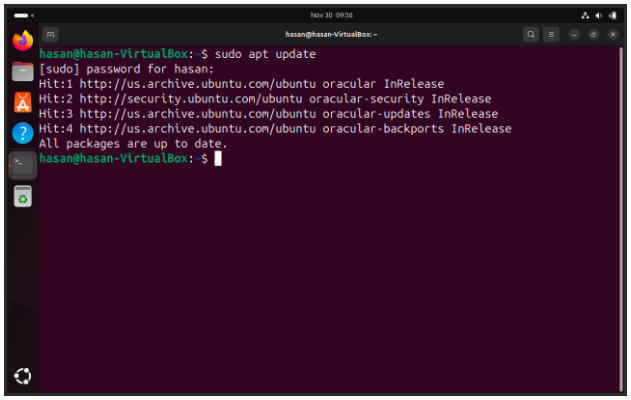

FIREWALL CONFIGURATION
VIRTUAL MACHINE
Ubuntu - Firewall (UFW)
DEFAULT POLICIES
Deny all incoming
Allow all outgoing
APPLICATION AND IP MANAGEMENT
Allow Wsdd
Allow 192.168.1.100, 192.168.1.0/24
Deny 203.0.113.0
SERVER ACCESS
curl http://10.0.2.15
ssh hasan@10.0.2.15
curl -Ik https://10.0.2.15
Allow 22/tcp
Allow 8080/ tcp, 1000-2000/ tcp
Deny 23/tcp
Allow HTTP
Allow HTTPS
Allow
Allow
Deny
Allow
Allow
External Network

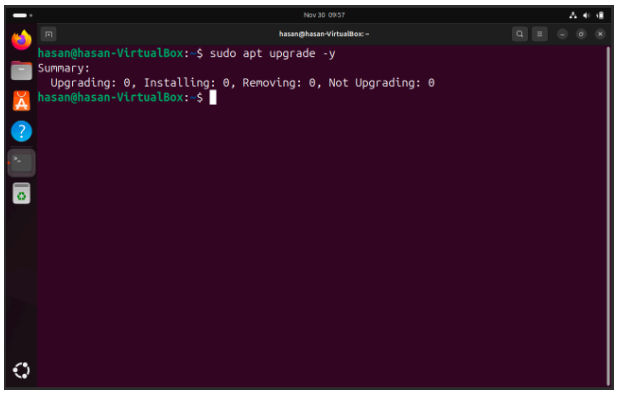

Name and Operating System
Name: Ubuntu - Firewall (UFW)
Folder: /Users/hasanwilliams/VirtualBox VMs
ISO Image: /Users/hasanwilliams/VirtualBox VMs/ubuntu-24.10-desktop-amd64.iso
Edition:
Type: Linux
Subtype: Ubuntu
Version: Ubuntu (64-bit)
Skip Unattended Installation
Unattended Install
Hardware
Hard Disk

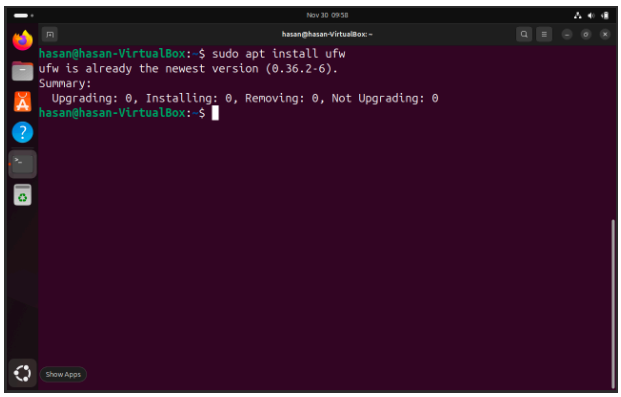

Name and Operating System
Unattended Install
Hardware
Base Memory: 4096 MB
4 MB
16384 MB
Processors: 1
1 CPU
16 CPUs
Enable EFI (special OSes only)
Hard Disk

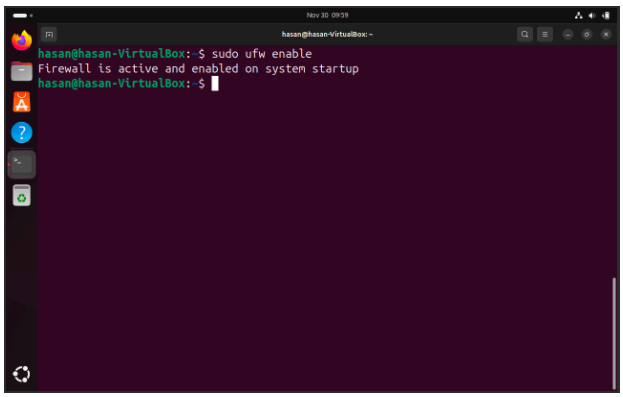

Name and Operating System
Unattended Install
Hardware
Hard Disk
Create a Virtual Hard Disk Now
Hard Disk File Location and Size
/Users/hasanwilliams/VirtualBox VMs/Ubuntu - Firewall (UFW)_/Ubuntu - Firewall (UFW)_.vdi
20.00 GB
4.00 MB
2.00 TB
Hard Disk File Type and Variant
VDI (VirtualBox Disk Image)
Pre-allocate Full Size
Split Into 2GB Parts
Use an Existing Virtual Hard Disk File
Kali.vdi (Normal, 20.00 GB)
Do Not Add a Virtual Hard Disk

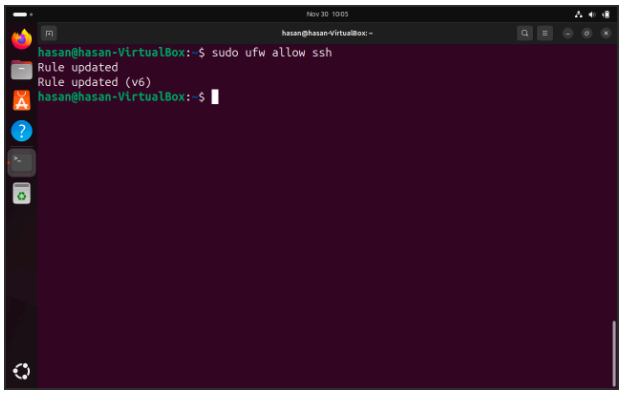

Ubuntu Firewall (UFW) [Running]
Next
Welcome to Ubuntu 24.10!
Complete your setup with additional settings and we'll have you up and running in no time
View release notes
Home

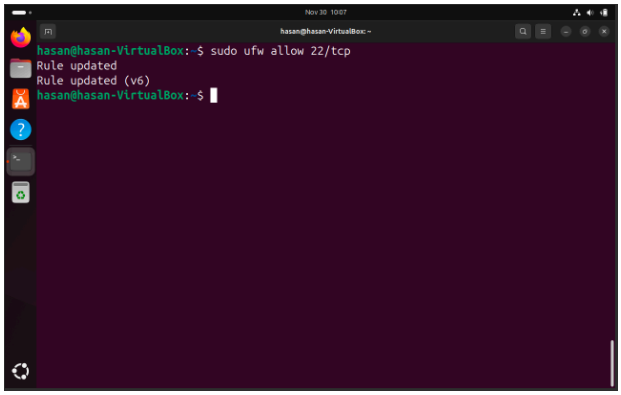

hasan@hasan-VirtualBox:~$ sudo apt update
[sudo] password for hasan:
Hit:1 http://us.archive.ubuntu.com/ubuntu oracular InRelease
Hit:2 http://security.ubuntu.com/ubuntu oracular-security InRelease
Hit:3 http://us.archive.ubuntu.com/ubuntu oracular-updates InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu oracular-backports InRelease
All packages are up to date.
hasan@hasan-VirtualBox:~$

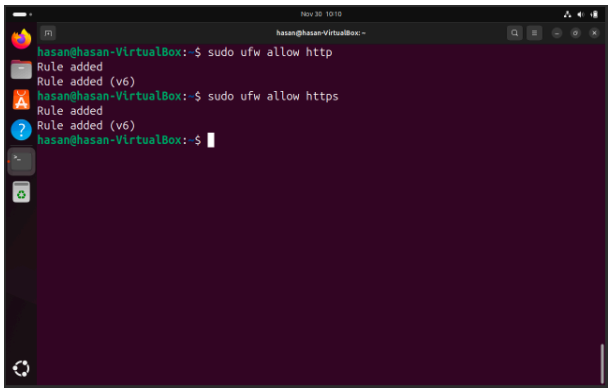

hasan@hasan-VirtualBox:~$ sudo apt upgrade -y
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
hasan@hasan-VirtualBox:~$

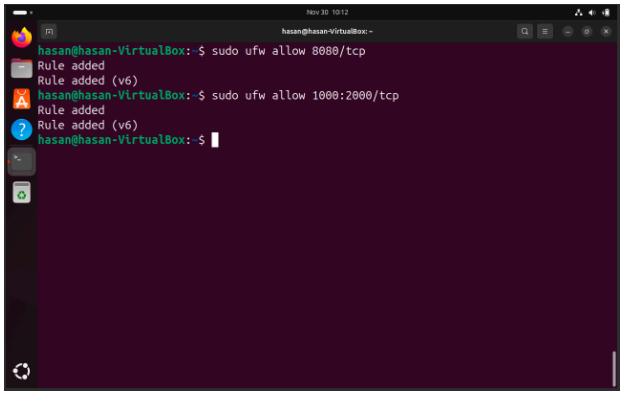

hasan@hasan-VirtualBox:~$ sudo apt install ufw
ufw is already the newest version (0.36.2-6).
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
hasan@hasan-VirtualBox:~$
Show Apps

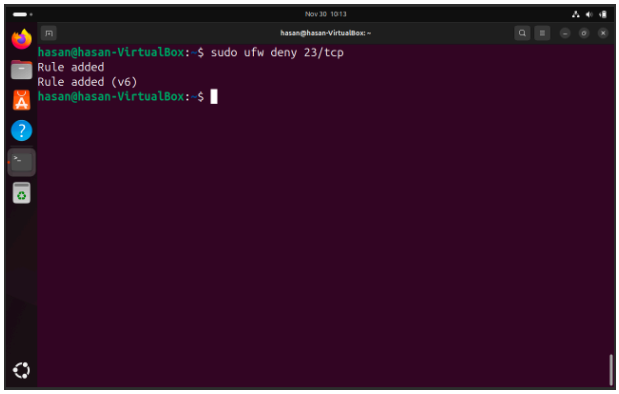

hasan@hasan-VirtualBox:~$ sudo ufw enable
Firewall is active and enabled on system startup
hasan@hasan-VirtualBox:~$


hasan@hasan-VirtualBox:~$ sudo ufw allow ssh
Rule updated
Rule updated (v6)
hasan@hasan-VirtualBox:~$

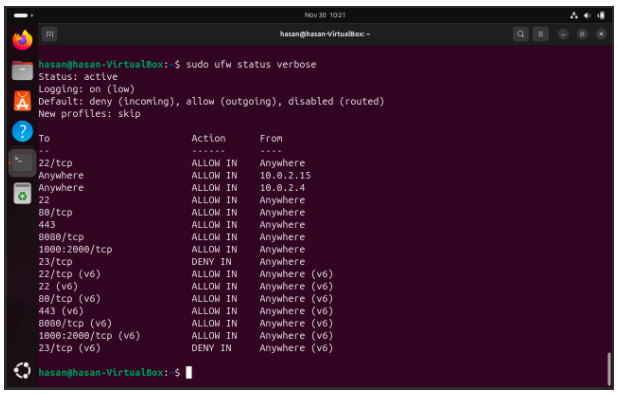

hasan@hasan-VirtualBox:~$ sudo ufw allow 22/tcp
Rule updated
Rule updated (v6)
hasan@hasan-VirtualBox:~$


hasan@hasan-VirtualBox:~$ sudo ufw allow http
Rule added
Rule added (v6)
hasan@hasan-VirtualBox:~$ sudo ufw allow https
Rule added
Rule added (v6)
hasan@hasan-VirtualBox:~$

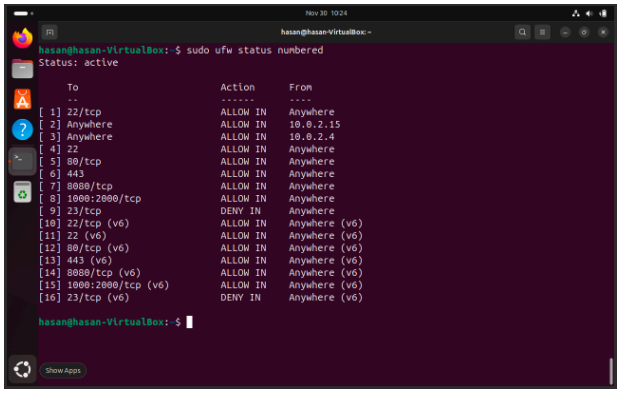

hasan@hasan-VirtualBox:~$ sudo ufw allow 8080/tcp
Rule added
Rule added (v6)
hasan@hasan-VirtualBox:~$ sudo ufw allow 1000:2000/tcp
Rule added
Rule added (v6)
hasan@hasan-VirtualBox:~$



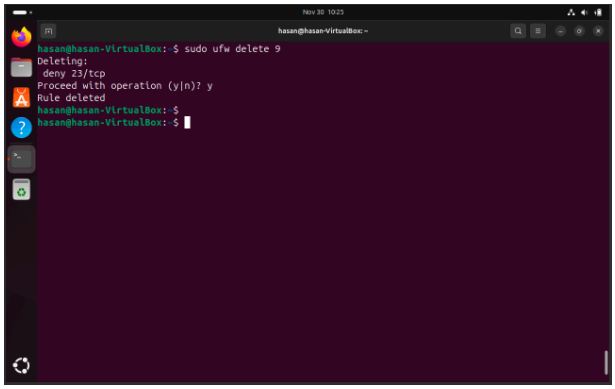
```
hasan@hasan-VirtualBox:~$ sudo ufw deny 23/tcp
Rule added
Rule added (v6)
hasan@hasan-VirtualBox:~$
```



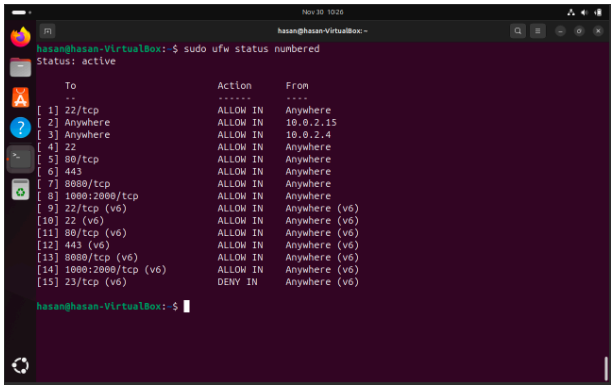
```
hasan@hasan-VirtualBox:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW IN    Anywhere
Anywhere                   ALLOW IN    10.0.2.15
Anywhere                   ALLOW IN    10.0.2.4
22                         ALLOW IN    Anywhere
80/tcp                     ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
8080/tcp                   ALLOW IN    Anywhere
1000:2000/tcp              ALLOW IN    Anywhere
23/tcp                     DENY IN     Anywhere
22/tcp (v6)                ALLOW IN    Anywhere (v6)
22 (v6)                    ALLOW IN    Anywhere (v6)
80/tcp (v6)                ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
8080/tcp (v6)              ALLOW IN    Anywhere (v6)
1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
23/tcp (v6)                DENY IN     Anywhere (v6)

hasan@hasan-VirtualBox:~$
```



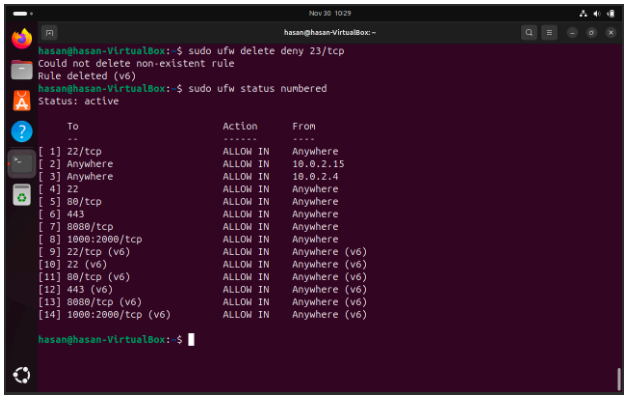
```
hasan@hasan-VirtualBox:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] Anywhere                   ALLOW IN    10.0.2.15
[ 3] Anywhere                   ALLOW IN    10.0.2.4
[ 4] 22                         ALLOW IN    Anywhere
[ 5] 80/tcp                     ALLOW IN    Anywhere
[ 6] 443                        ALLOW IN    Anywhere
[ 7] 8080/tcp                   ALLOW IN    Anywhere
[ 8] 1000:2000/tcp              ALLOW IN    Anywhere
[ 9] 23/tcp                     DENY IN     Anywhere
[10] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[11] 22 (v6)                    ALLOW IN    Anywhere (v6)
[12] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[13] 443 (v6)                   ALLOW IN    Anywhere (v6)
[14] 8080/tcp (v6)              ALLOW IN    Anywhere (v6)
[15] 1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
[16] 23/tcp (v6)                DENY IN     Anywhere (v6)

hasan@hasan-VirtualBox:~$
```



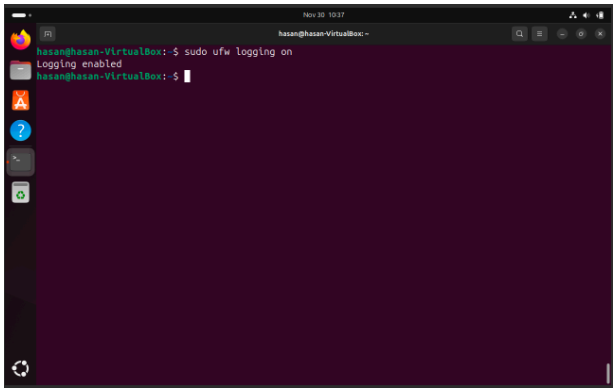
```
hasan@hasan-VirtualBox:~$ sudo ufw delete 9
Deleting:
 deny 23/tcp
Proceed with operation (y|n)? y
Rule deleted
hasan@hasan-VirtualBox:~$
hasan@hasan-VirtualBox:~$
```

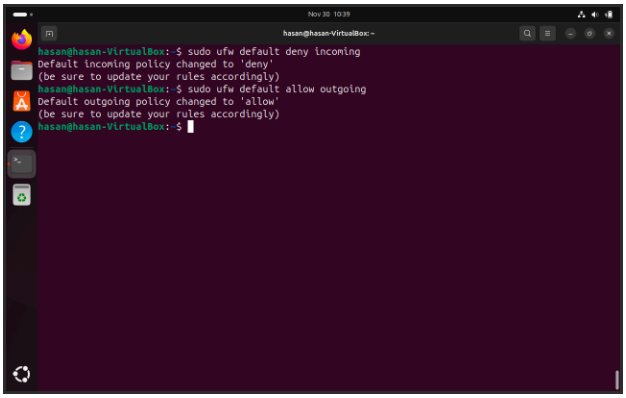


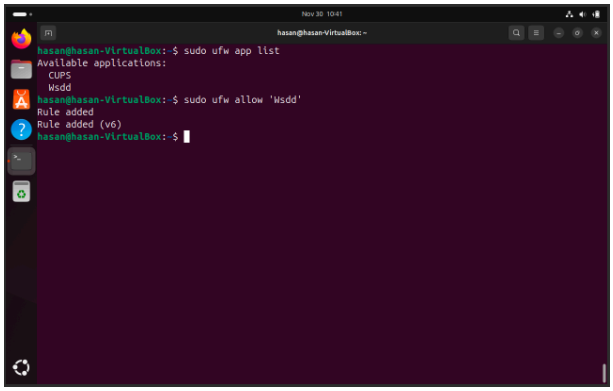
```
hasan@hasan-VirtualBox:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] Anywhere                   ALLOW IN    10.0.2.15
[ 3] Anywhere                   ALLOW IN    10.0.2.4
[ 4] 22                         ALLOW IN    Anywhere
[ 5] 80/tcp                     ALLOW IN    Anywhere
[ 6] 443                        ALLOW IN    Anywhere
[ 7] 8080/tcp                   ALLOW IN    Anywhere
[ 8] 1000:2000/tcp              ALLOW IN    Anywhere
[ 9] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[10] 22 (v6)                    ALLOW IN    Anywhere (v6)
[11] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[12] 443 (v6)                   ALLOW IN    Anywhere (v6)
[13] 8080/tcp (v6)              ALLOW IN    Anywhere (v6)
[14] 1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)
[15] 23/tcp (v6)                DENY IN     Anywhere (v6)

hasan@hasan-VirtualBox:~$
```

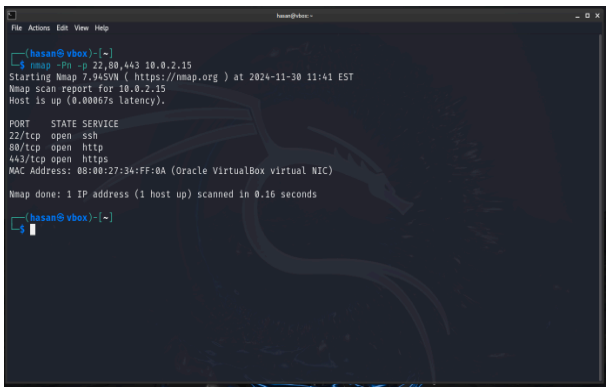


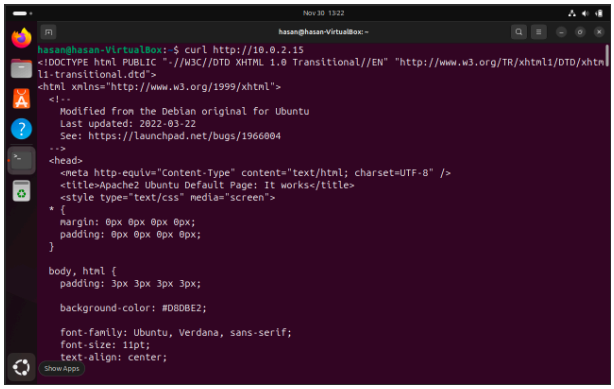
```
hasan@hasan-VirtualBox:~$ sudo ufw delete deny 23/tcp
Could not delete non-existent rule
Rule deleted (v6)
hasan@hasan-VirtualBox:~$ sudo ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 22/tcp                     ALLOW IN    Anywhere
[ 2] Anywhere                   ALLOW IN    10.0.2.15
[ 3] Anywhere                   ALLOW IN    10.0.2.4
[ 4] 22                         ALLOW IN    Anywhere
[ 5] 80/tcp                     ALLOW IN    Anywhere
[ 6] 443                        ALLOW IN    Anywhere
[ 7] 8080/tcp                   ALLOW IN    Anywhere
[ 8] 1000:2000/tcp              ALLOW IN    Anywhere
[ 9] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
[10] 22 (v6)                    ALLOW IN    Anywhere (v6)
[11] 80/tcp (v6)                ALLOW IN    Anywhere (v6)
[12] 443 (v6)                   ALLOW IN    Anywhere (v6)
[13] 8080/tcp (v6)              ALLOW IN    Anywhere (v6)
[14] 1000:2000/tcp (v6)         ALLOW IN    Anywhere (v6)

hasan@hasan-VirtualBox:~$
```

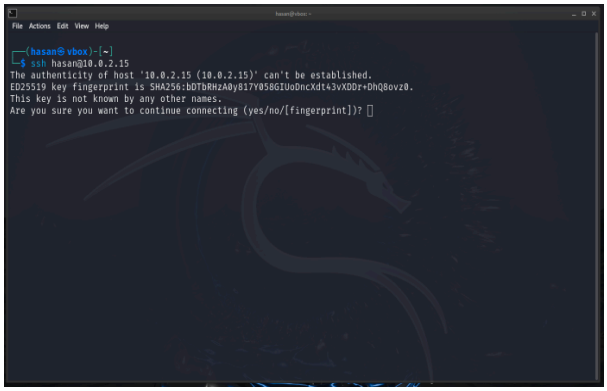

Nov 30 10:37
hasan@hasan-VirtualBox: ~
hasan@hasan-VirtualBox:~$ sudo ufw logging on
Logging enabled
hasan@hasan-VirtualBox:~$

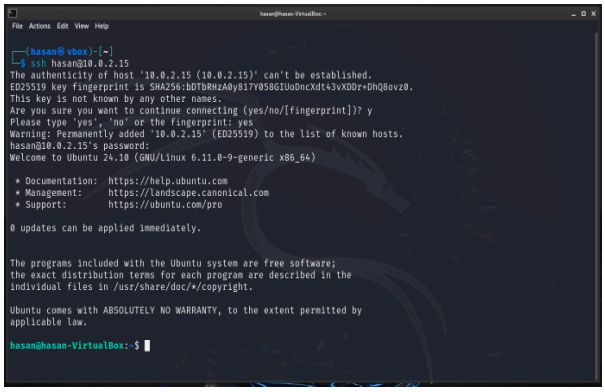

Nov 30 10:39
hasan@hasan-VirtualBox: ~
hasan@hasan-VirtualBox:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
hasan@hasan-VirtualBox:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
hasan@hasan-VirtualBox:~$

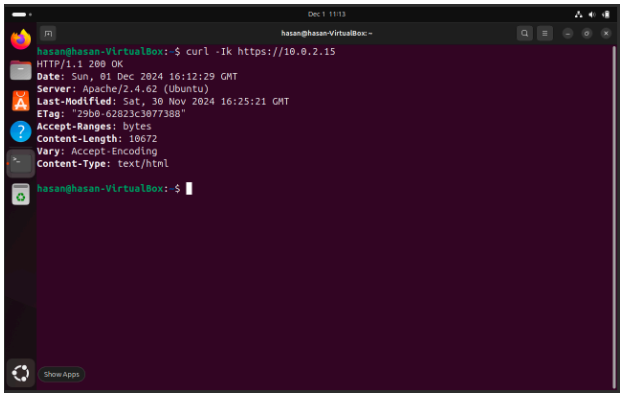

Nov 30 10:41
hasan@hasan-VirtualBox: ~
hasan@hasan-VirtualBox:~$ sudo ufw app list
Available applications:
CUPS
Wsdd
hasan@hasan-VirtualBox:~$ sudo ufw allow 'Wsdd'
Rule added
Rule added (v6)
hasan@hasan-VirtualBox:~$


File Actions Edit View Help
(hasan㉿vbox)-[~]
$ nmap -Pn -p 22,80,443 10.0.2.15
Starting Nmap 7.945VN (https://nmap.org) at 2024-11-30 11:41 EST
Nmap scan report for 10.0.2.15
Host is up (0.00067s latency).
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https
MAC Address: 08:00:27:34:FF:0A (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
(hasan㉿vbox)-[~]
$


Nov 30 13:22
hasan@hasan-VirtualBox: ~
hasan@hasan-VirtualBox:~$ curl http://10.0.2.15
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<!--
Modified from the Debian original for Ubuntu
Last updated: 2022-03-22
See: https://launchpad.net/bugs/1966004
-->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Ubuntu Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}
body, html {
padding: 3px 3px 3px 3px;
background-color: #D8DBE2;
font-family: Ubuntu, Verdana, sans-serif;
font-size: 11pt;
text-align: center;
Show Apps


File Actions Edit View Help
(hasan㉿vbox)-[~]
$ ssh hasan@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:bDTbRHzA0y817Y058GIUoDncXdt43vXODr+DhQ8ovz0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?


File Actions Edit View Help
(hasan㉿vbox)-[~]
$ ssh hasan@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:bDTbRHzA0y817Y058GIUoDncXdt43vXODr+DhQ8ovz0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
hasan@10.0.2.15's password:
Welcome to Ubuntu 24.10 (GNU/Linux 6.11.0-9-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro
0 updates can be applied immediately.
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
hasan@hasan-VirtualBox:~$


Dec 1 11:13
hasan@hasan-VirtualBox: ~
hasan@hasan-VirtualBox:~$ curl -Ik https://10.0.2.15
HTTP/1.1 200 OK
Date: Sun, 01 Dec 2024 16:12:29 GMT
Server: Apache/2.4.62 (Ubuntu)
Last-Modified: Sat, 30 Nov 2024 16:25:21 GMT
ETag: "29b0-62823c3077388"
Accept-Ranges: bytes
Content-Length: 10672
Vary: Accept-Encoding
Content-Type: text/html
hasan@hasan-VirtualBox:~$
Show Apps