

Low Level Implementation Report

Final Low Level Design and Functional Testng Report

Prepared For:

Marc Hayes

Seneca Polytechnic

Prepared By:

Ornan Roberts

Ramachandra Muralidhara

Syed Mujahid Hamid Ali

Yannish Kumar Ballachandher Sreedevi

December 11, 2023

Table of Contents

Executive Summary	3
System Overview	3
About Company	3
Business Requirements	3
Business Applications	4
System Design	4
Zones Segmentation	4
System Components	5
Software	5
Hardware	7
Security Controls	7
Functional Testing	8
Secured Website	8
Root Website	8
E-Commerce	9
Secured Website (FTP/Nextcloud)	9
Web Application Firewall	10
Backup Script	11
DNS	12
Private DNS	12
Public DNS	12
Database	13
FTP/Nextcloud Docker Compose	13
Web Servers	13
Firewall configurations	14
VPN Configuration	15
Server Configuration File	16
Client Configuration File	16
Using Ubuntu UI to add VPN Configuration File on the Client	17
Selecting the Configuration File	17
Adding the right certificates and other files	18
Tunnel interface created on Client when VPN is turned on	18
Tunnel interface on the Server	19
Successful ping attempt made from Client to Server	19
Conclusion	20

Executive Summary

The low-level implementation report for the Agricore infrastructure which is an ecommerce business. The report outlines various aspects of the system and business covering different requirements. The business requirements are meticulously outlined to emphasize the need for a secure e-commerce website. We perform implementation of security controls based on industry standards. The hardware and software components are strategically deployed to create a resilient and scalable architecture. Lastly, we performed functional testing which ensures that the implemented features align with the defined business requirements.

System Overview

About Company

Agricore is a thriving agriculture tools e-commerce business dedicated to providing farmers, growers, and enthusiasts with top-quality tools and equipment to optimize their farming practices. We are committed to leveraging technology for the advancement of agriculture. By integrating innovative solutions, promoting sustainability, and prioritizing cybersecurity, we aim to provide a safe and secure digital platform for the agriculture tools industry, driving positive change for farmers and the environment. The company profile is based on small to medium sized approx 100 people based from a single office.

Business Requirements

1. An e-commerce website with secure payment processing capabilities using strong encryption standards for online sales of agricultural tools.
2. Create a comprehensive products catalog that categorizes tools based on type.
3. Implement a user-friendly content management system for managing product listings, content, and promotions.
4. Add user registration and login functionality for order tracking and preferences.
5. Authentication in order to prevent any unauthorized access and strong password policies.
6. Ensure privacy policy outlines how consumers data will be collected, used and matches the Canadian privacy standards i.e PCI DSS.
7. Protect customer data by securely storing it in a protected database.
8. Ensure firewalls and security products are added to infrastructure to protect against cyber threats.
9. Develop a backup and recovery plan for all core and mission critical applications/services.

10. Web application security should be implemented on web servers to detect and handle requests.
11. Infrastructure consists of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to protect against cyber threats.
12. Infrastructure maintains high availability and redundancy to decrease downtime.
13. Security policies and procedures for internal network and external users to protect the network infrastructure.

Business Applications

The applications and softwares required for a business can vary depending on the processes involved in the operation. The following is a list of essential business applications for technical and functional requirements.

1. Apache Web Service
2. WordPress CMS
3. MySQL Database
4. pfSense
5. SFTP
6. Bind9
7. Nextcloud
8. Web Application Firewall

System Design

Zones Segmentation

DMZ Zone: The DMZ zone stands for demilitarized zones because it consists of services and applications that are available to the public and are public facing such as web servers. The DMZ is usually in between layers of security which serves requests from external connections. It also filters and monitors the traffic from outside to protect the internal infrastructure. This zone plays a pivotal role in enhancing security by isolating public-facing services from the internal network while allowing controlled and monitored access. The devices within this include the web servers, external DNS server, public host container, web application firewall and IDS.

Internal Zone: This is the internal zone and is the core of the organization. All trusted services and applications along with sensitive data and servers are usually located within this zone. The internal zone has a lot of security and is a restricted zone with no outside connections. It is crucial to have network monitoring policies within the

assets in this zone to protect the internal infrastructure. The devices that are in this zone include the private container host, FTP server, and internal workstations.

Administration Zone: This is the most critical zone within the infrastructure where all the infrastructure backbone is placed. Administrative access is only required within this zone for maintenance and troubleshooting. The devices in this zone are important for the correct working of the network and overall infrastructure. This zone includes servers such as internal DNS, AD server, DHCP, backup server and administrator PC.

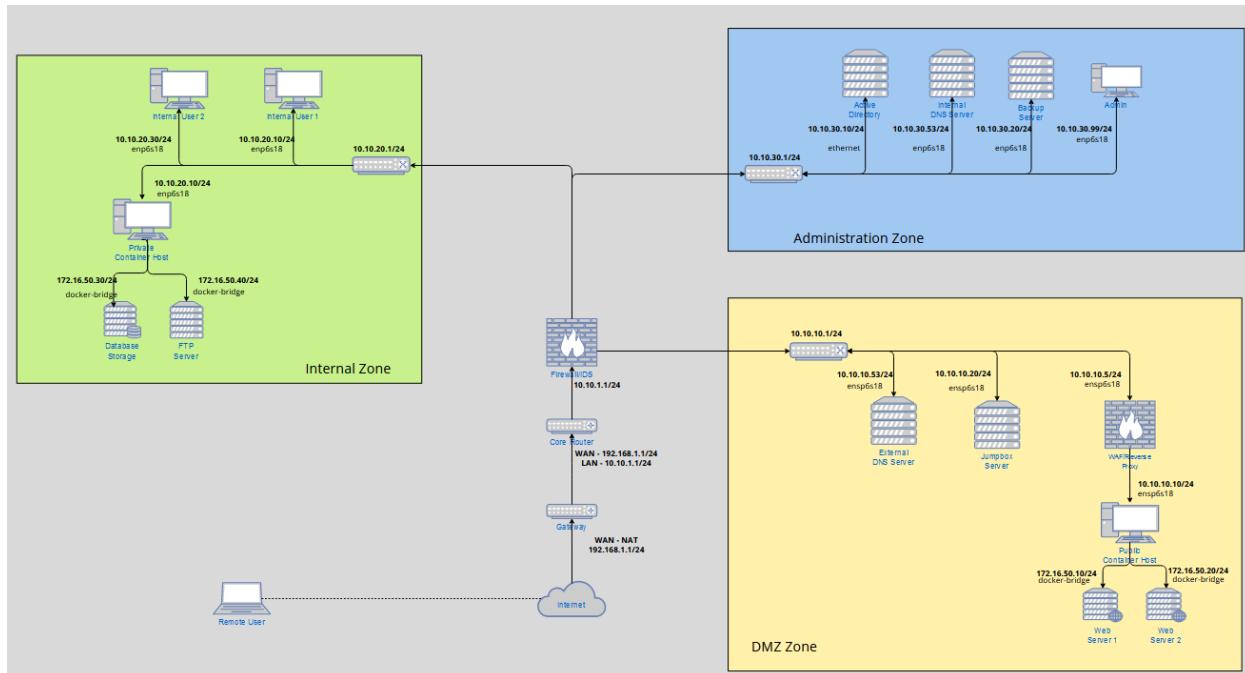


Fig.1 Network Design with zones segmentation

System Components

The following are the hardware and software assets which are critical components for the infrastructure.

Software

Asset Name	Role	OS	Software	Version
Gateway Router	Edge router connecting to internet and domain	FreeBSD	pfsense	2.7
Core Router	Internal router performing	FreeBSD	pfsense	2.7

	internal routing activity.			
Firewall	Monitoring and filtering traffic within the domain	FreeBSD	pfsense	2.7
IDS	Acts as monitoring server to log events and traffic	Ubuntu	Snort	3.1
Web Application Firewall/Reverse Proxy	Protection for web server against web attacks	Ubuntu	Modsecurity	3.0.10
AD Server	Domain controller and server for managing users and computers	Microsoft Windows Server	Active Directory Domain Services	2019
Internal DNS Server	Resolve DNS queries for internal connections	Ubuntu	Bind9	22.04
External DNS Server	Resolve DNS queries for external connections	Ubuntu	Bind9	22.04
DHCP Server	Assign IP addresses to computers within the domain	FreeBSD	pfsense	2.7
Database Server	MySQL server to store web content data.	Ubuntu	MySQL	22.04
FTP Server	File sharing service for internal	Container	NextCloud	2.6

	communication			
Web Server 1 & 2	Web servers for e-commerce activities	Container	Wordpress	6.3.1
Backup Server	Backing up information related to web content	Ubuntu	Rsync	3.2
Container Hosts (public and private)	Container running docker images for infrastructure services	Ubuntu	Docker	22.04
Internal User	Employee workstations	Windows	Windows	10
Admin PC	Administrator workstation for IT maintenance	Ubuntu	-	22.04

Hardware

Asset Name	Role	OS	Software	Version
Home Lab Server	Infrastructure deployed to the server	Debian 12	Proxmox	8.0.3

Security Controls

Security controls are critical within the infrastructure as these measures are put in place to protect information, systems, assets, and organizations from various threats and risks. Based on industry standards that meet the requirements for businesses the necessary security controls were implemented onto the topology. CIS Controls were used as reference.

- Inventory Control of Software Assets
- Account Management
- Access Control Management
- Audit Log Management
- Email and Web Browser Protection
- Malware Defense

- Data Recovery
- Network Monitoring and Defense

Functional Testing

Functional testing is a critical phase in designing the infrastructure that focuses on verifying that the system or application behaves according to specified requirements. Testing was performed by ensuring that we meet the business requirements of the system. As per the business requirements we added the necessary functionalities that have been showcased below.

Secured Website

Root Website

All web servers hosting the Agricore website were running SSL where certificates were created and added. The public and private web servers were both running SSL ensuring a safe and encrypted connection.

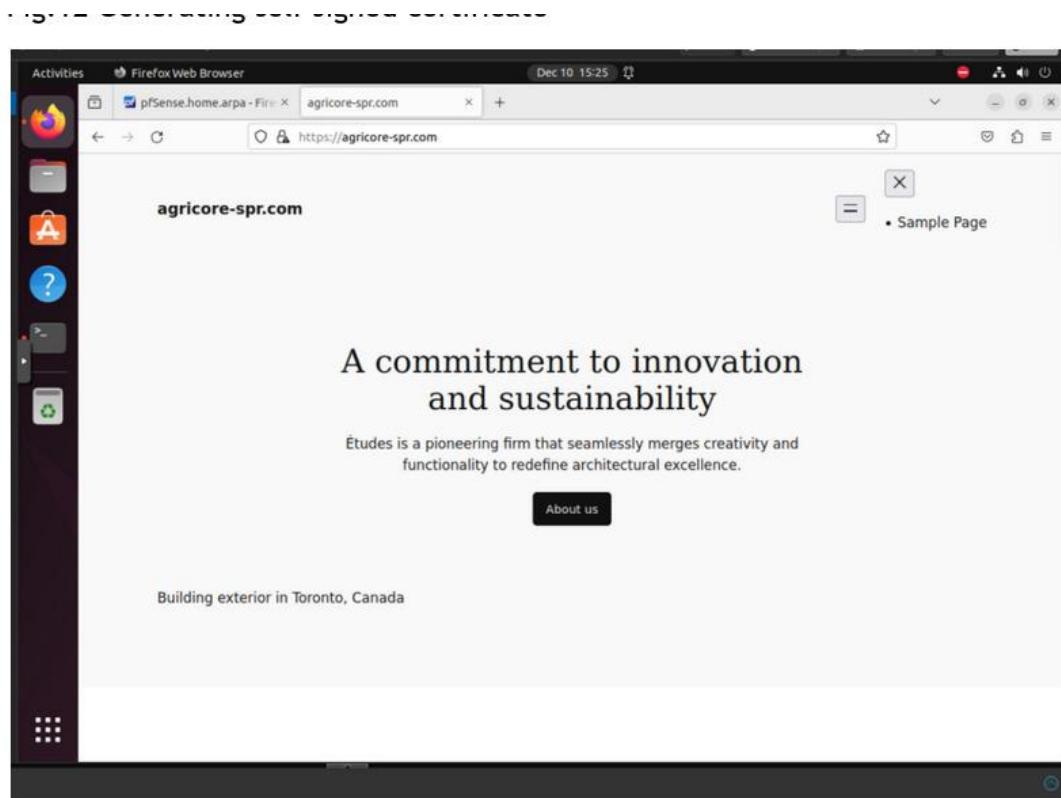


Fig.13 SSL certificate added and site with https

E-Commerce

The screenshot shows a Firefox browser window with multiple tabs open. The active tab displays the URL <https://web2.agricore-spr.com/#>. The page content is a dark-themed "My eCommerce Store" interface with a navigation bar (Home, Shop, Categories) and some placeholder text. A "Page Info" dialog is overlaid on the page, specifically for the URL above. The "Security" tab is selected in the dialog. Key details shown include:

- Website Identity**: Website: web2.agricore-spr.com, Owner: This website does not supply ownership information. Verified by: Agricore.
- Privacy & History**: Have I visited this website prior to today? No. Is this website storing information on my computer? Yes, cookies. Have I saved any passwords for this website? No.
- Technical Details**: Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3). The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

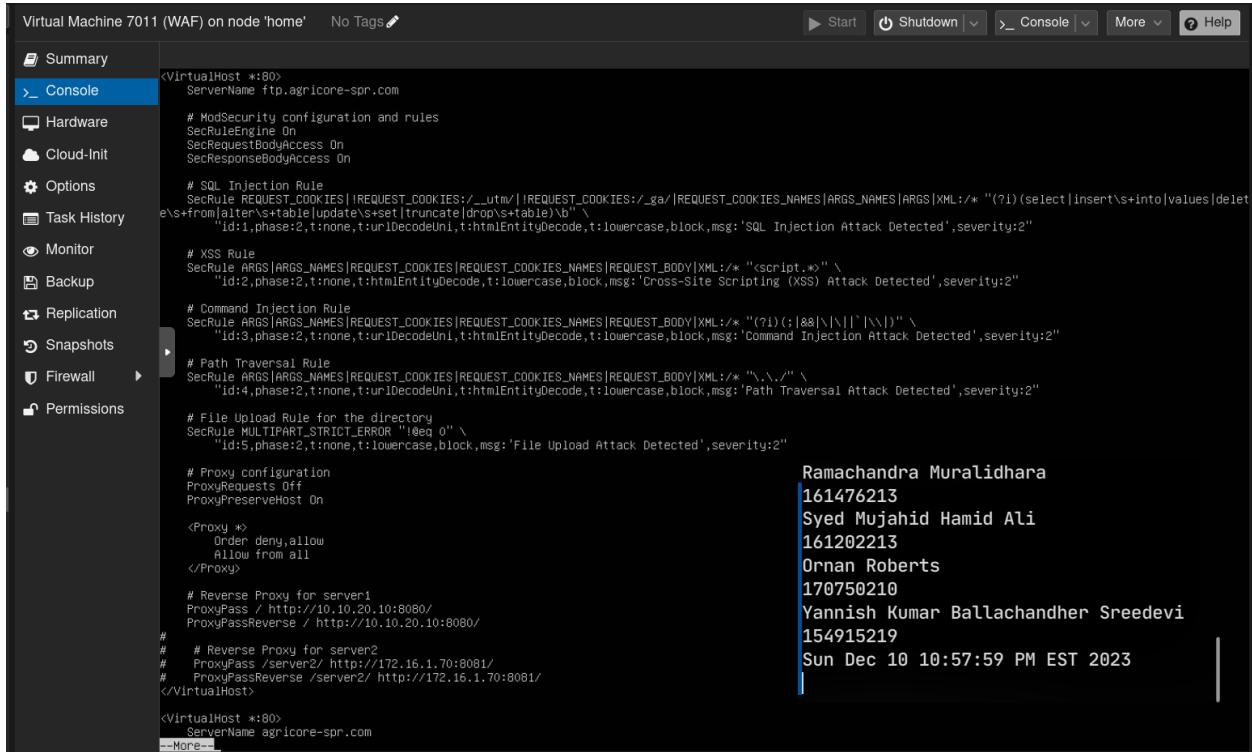
Secured Website (FTP/Nextcloud)

The screenshot shows a Firefox browser window with multiple tabs open. The active tab displays the URL <https://ftp.agricore-spr.com/apps/files/?dir=/&fileid=2>. The page content is a Nextcloud file manager interface showing a list of files in a folder. A "Page Info" dialog is overlaid on the page, specifically for the URL above. The "Security" tab is selected in the dialog. Key details shown include:

- Website Identity**: Website: ftp.agricore-spr.com, Owner: This website does not supply ownership information. Verified by: Agricore.
- Privacy & History**: Have I visited this website prior to today? No. Is this website storing information on my computer? Yes, cookies and 16.0 kB of site data. Have I saved any passwords for this website? No.
- Technical Details**: Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3). The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it difficult for unauthorized people to view information travelling between computers. It is therefore unlikely that anyone read this page as it travelled across the network.

Web Application Firewall

Web Application Firewall is a crucial component of web application security infrastructure, providing proactive defense against a wide array of threats and vulnerabilities. WAF was implemented using Modsecurity and the rules were created to protect against web based attacks such cross-site scripting, SQL injection, proxy.

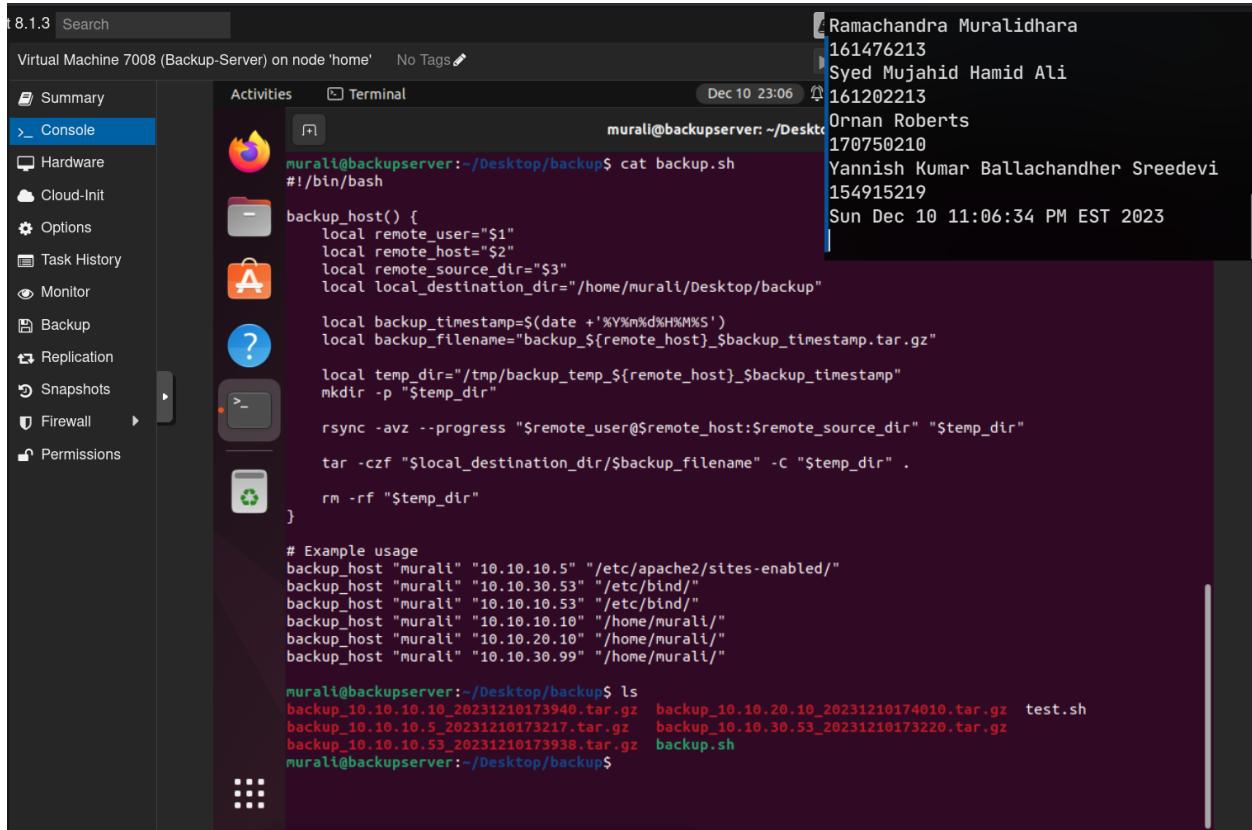


The screenshot shows a terminal window titled "Virtual Machine 7011 (WAF) on node 'home'" with the "Console" tab selected. The window contains a large amount of ModSecurity configuration code. A vertical scroll bar is visible on the right side of the terminal window. The configuration includes rules for SQL Injection, XSS, Command Injection, Path Traversal, File Upload, and Proxy settings. On the right side of the terminal window, there is a list of names and IDs:

Ramachandra Muralidhara
161476213
Syed Mujahid Hamid Ali
161202213
Ornan Roberts
170750210
Yannish Kumar Ballachandher Sreedevi
154915219
Sun Dec 10 10:57:59 PM EST 2023

Backup Script

The backup plan was initiated using a script which backup configurations using rsync.
The script is designed to save files onto local admin pc.



The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, a sidebar lists various management options like Summary, Console, Hardware, Cloud-Init, Options, Task History, Monitor, Backup, Replication, Snapshots, Firewall, and Permissions. The 'Console' tab is currently selected. In the main pane, there's an 'Activities' section with several icons (File, Terminal, etc.) and a 'Terminal' section where a user named 'murali' is running a script named 'backup.sh'. The terminal output shows the script's logic for backing up files from multiple hosts to a local destination. At the bottom of the terminal window, it shows the command 'ls' has been run, listing several tar.gz files generated by the backup process. The top right corner of the screen shows a list of users with their last logins: Ramachandra Muralidhara (161476213), Syed Mujahid Hamid Ali (161202213), Ornan Roberts (170750210), and Yannish Kumar Ballachandher Sreedevi (154915219). The date and time displayed are Sun Dec 10 11:06:34 PM EST 2023.

```
murali@backupserver:~/Desktop/backup$ cat backup.sh
#!/bin/bash

backup_host() {
    local remote_user="$1"
    local remote_host="$2"
    local remote_source_dir="$3"
    local local_destination_dir="/home/murali/Desktop/backup"

    local backup_timestamp=$(date '+%Y%m%d%H%M%S')
    local backup_filename="backup_${remote_host}_${backup_timestamp}.tar.gz"
    local temp_dir="/tmp/backup_temp_${remote_host}_${backup_timestamp}"
    mkdir -p "$temp_dir"

    rsync -avz --progress "$remote_user@$remote_host:$remote_source_dir" "$temp_dir"
    tar -czf "$local_destination_dir/$backup_filename" -C "$temp_dir" .

    rm -rf "$temp_dir"
}

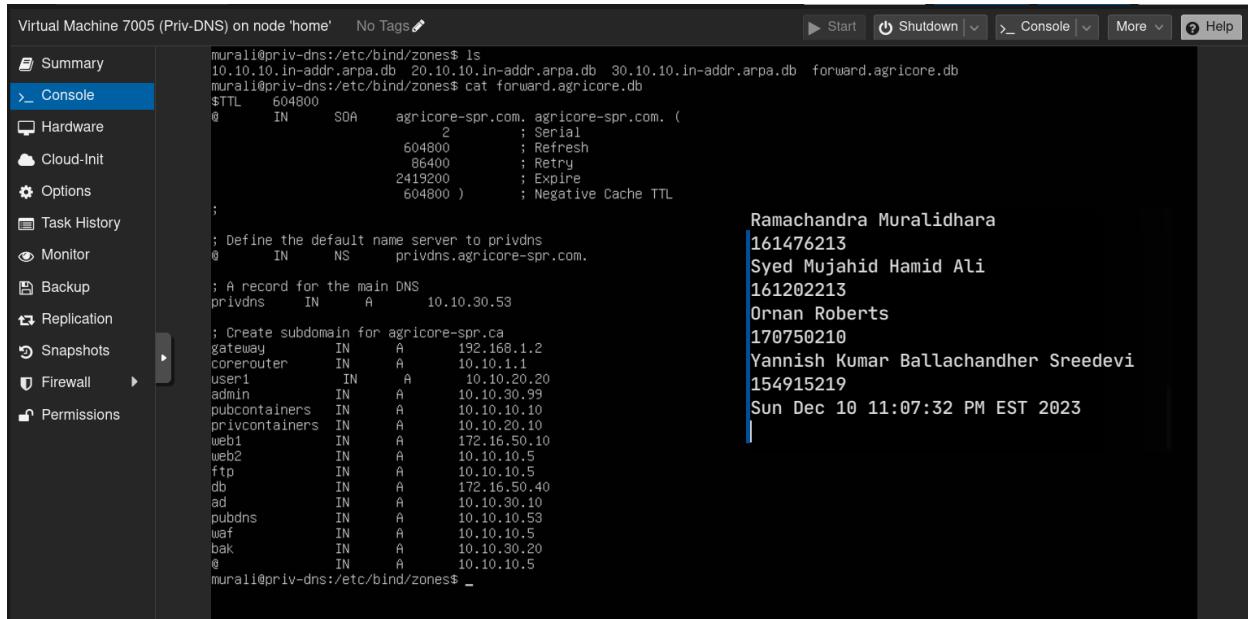
# Example usage
backup_host "murali" "10.10.10.5" "/etc/apache2/sites-enabled/"
backup_host "murali" "10.10.30.53" "/etc/bind/"
backup_host "murali" "10.10.10.53" "/etc/bind/"
backup_host "murali" "10.10.10.10" "/home/murali/"
backup_host "murali" "10.10.20.10" "/home/murali/"
backup_host "murali" "10.10.30.99" "/home/murali/"

murali@backupserver:~/Desktop/backup$ ls
backup_10.10.10.20231210173940.tar.gz  backup_10.10.20.10_20231210174010.tar.gz  test.sh
backup_10.10.10.5_20231210173217.tar.gz  backup_10.10.30.53_20231210173220.tar.gz
backup_10.10.53_20231210173938.tar.gz  backup.sh
```

DNS

BIND9 operates as a DNS server, responding to DNS queries from clients by resolving domain names. Private and public DNS servers were added, resolving queries for public and private usage.

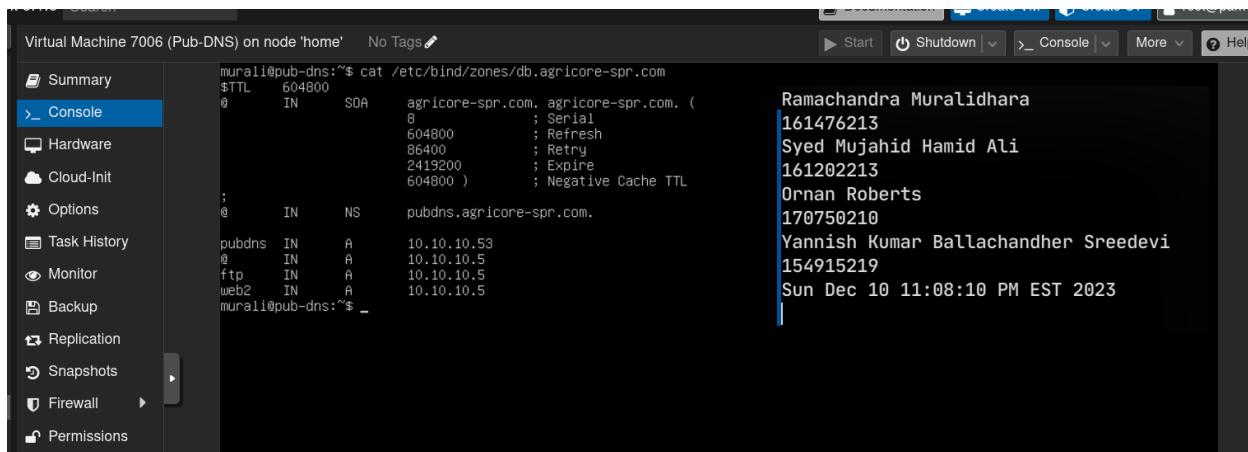
Private DNS



The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, a sidebar lists various settings like Summary, Console, Hardware, Cloud-Init, Options, Task History, Monitor, Backup, Replication, Snapshots, Firewall, and Permissions. The 'Console' tab is selected. In the main pane, a terminal window displays the contents of the /etc/bind/zones/db file. The file contains an SOA record for agricore-spr.com and numerous A records for subdomains and hosts within the network. To the right of the terminal, a list of names and their corresponding IP addresses is shown:

Name	IP Address
Ramachandra Muralidhara	161476213
Syed Mujahid Hamid Ali	161202213
Ornan Roberts	170750210
Yannish Kumar Ballachandher Sreedevi	154915219
	Sun Dec 10 11:07:32 PM EST 2023

Public DNS



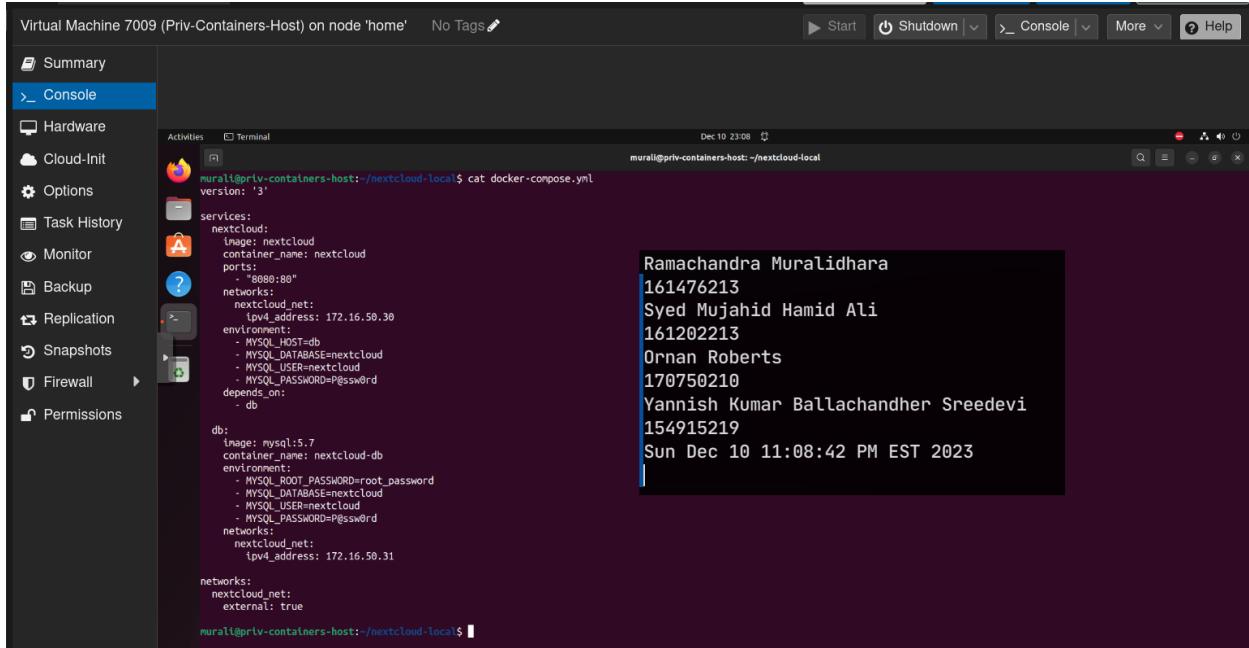
The screenshot shows the Oracle VM VirtualBox Manager interface, similar to the previous one. The 'Console' tab is selected in the sidebar. The terminal window shows the contents of the /etc/bind/zones/db/agricore-spr.com file. It includes an SOA record and A records for various hosts. To the right, a list of names and their IP addresses is displayed:

Name	IP Address
Ramachandra Muralidhara	161476213
Syed Mujahid Hamid Ali	161202213
Ornan Roberts	170750210
Yannish Kumar Ballachandher Sreedevi	154915219
	Sun Dec 10 11:08:10 PM EST 2023

Database

MySQL is an open-source DBMS that was implemented to store the data for web servers. The database server was initiated on a private docker container.

FTP/Nextcloud Docker Compose



The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, a sidebar lists various management options like Summary, Console, Hardware, Cloud-Init, Options, Task History, Monitor, Backup, Replication, Snapshots, Firewall, and Permissions. The 'Console' tab is currently selected. In the main pane, there's an 'Activities' section with a terminal icon and a 'Terminal' section. The terminal window has a title bar 'Virtual Machine 7009 (Priv-Containers-Host) on node 'home'' and a status bar 'Dec 10 23:08'. It displays the command 'cat docker-compose.yml' and its output:

```
murali@priv-containers-host:~/nextcloud-local$ cat docker-compose.yml
version: '3'

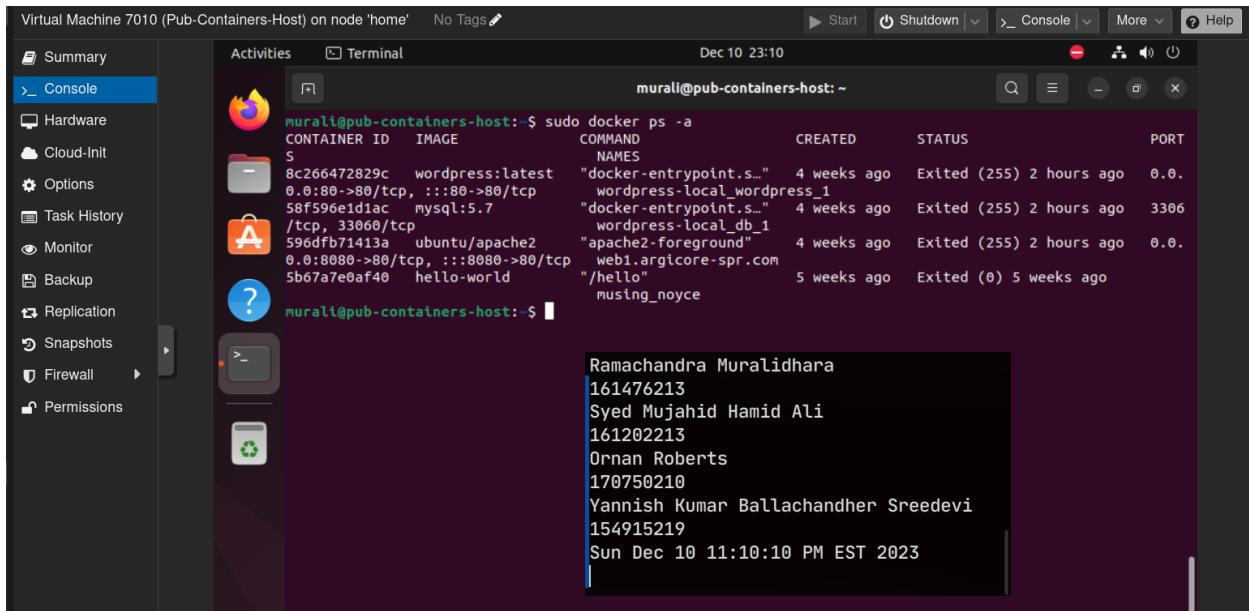
services:
  nextcloud:
    image: nextcloud
    container_name: nextcloud
    ports:
      - "8080:80"
    networks:
      nextcloud_net:
        ipv4_address: 172.16.50.30
    environment:
      - MYSQL_HOST=db
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud
      - MYSQL_PASSWORD=@pssw0rd
    depends_on:
      - db

  db:
    image: mysql:5.7
    container_name: nextcloud-db
    environment:
      - MYSQL_ROOT_PASSWORD=root_password
      - MYSQL_DATABASE=nextcloud
      - MYSQL_USER=nextcloud
      - MYSQL_PASSWORD=@pssw0rd
    networks:
      nextcloud_net:
        external: true

networks:
  nextcloud_net:
    external: true

murali@priv-containers-host:~/nextcloud-local$
```

Web Servers



The screenshot shows the Oracle VM VirtualBox Manager interface, similar to the previous one but for a different virtual machine. The sidebar and terminal window are identical. The terminal window shows the command 'sudo docker ps -a' and its output:

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORT
8c266472829c	wordpress:latest	"docker-entrypoint.s..."	4 weeks ago	Exited (255)	2 hours ago 0.0.0.0:80->80/tcp, :::80->80/tcp
58f596e1diac	mysql:5.7	"docker-entrypoint.s..."	4 weeks ago	Exited (255)	2 hours ago 3306/tcp, 33060/tcp
596dfb71413a	ubuntu/apache2	"apache2-foreground"	4 weeks ago	Exited (255)	2 hours ago 0.0.0.0:8080->80/tcp, :::8080->80/tcp
5b67a7e0af40	hello-world	"hello"	5 weeks ago	Exited (0)	5 weeks ago musing_noxyce

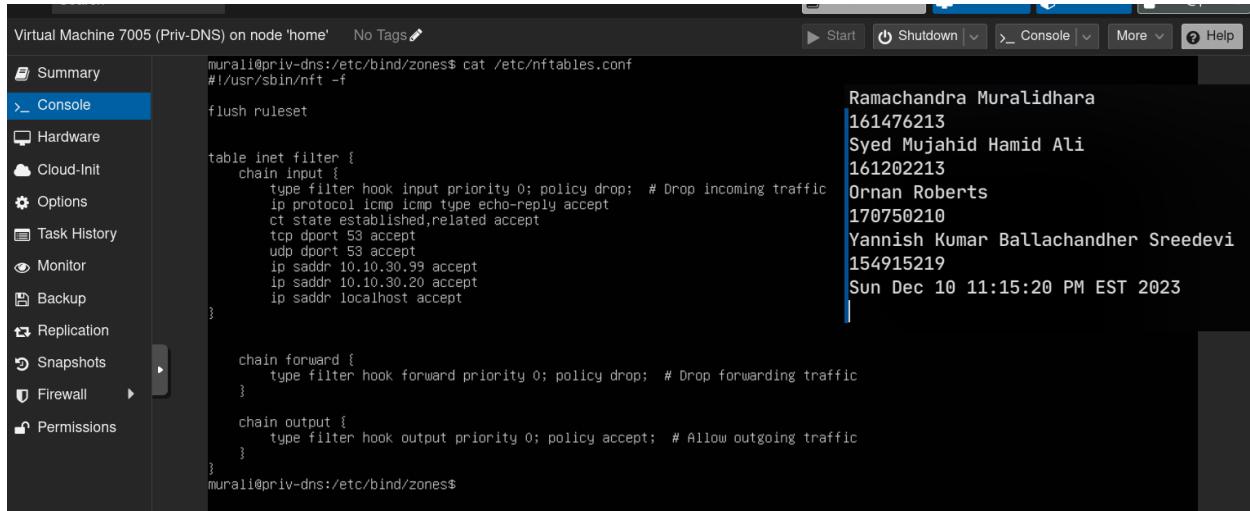
Below the terminal window, a message box displays the names and IDs of several team members:

```
Ramachandra Muralidhara
161476213
Syed Mujahid Hamid Ali
161202213
Ornan Roberts
170750210
Yannish Kumar Ballachandher Sreedevi
154915219
Sun Dec 10 11:10:10 PM EST 2023
```

Firewall configurations

Host Based

Private DNS



The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, a sidebar lists various settings like Summary, Console, Hardware, Cloud-Init, Options, Task History, Monitor, Backup, Replication, Snapshots, Firewall, and Permissions. The 'Firewall' option is selected. In the main pane, a terminal window is open with the command `cat /etc/nftables.conf`. The output of this command is displayed on the right side of the terminal window. The configuration includes rules for the 'filter' table's 'inet' chain, specifically for 'input', 'forward', and 'output' chains. It drops incoming traffic (except for ICMP echo-reply) and allows outgoing traffic (including DNS traffic on port 53). A list of names and their corresponding IDs is also present on the right.

```
murali@priv-dns:/etc/bind/zones$ cat /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0; policy drop; # Drop incoming traffic
        ip protocol icmp icmp type echo-reply accept
        ct state established,related accept
        tcp dport 53 accept
        udp dport 53 accept
        ip saddr 10.10.30.99 accept
        ip saddr 10.10.30.20 accept
        ip saddr localhost accept
    }

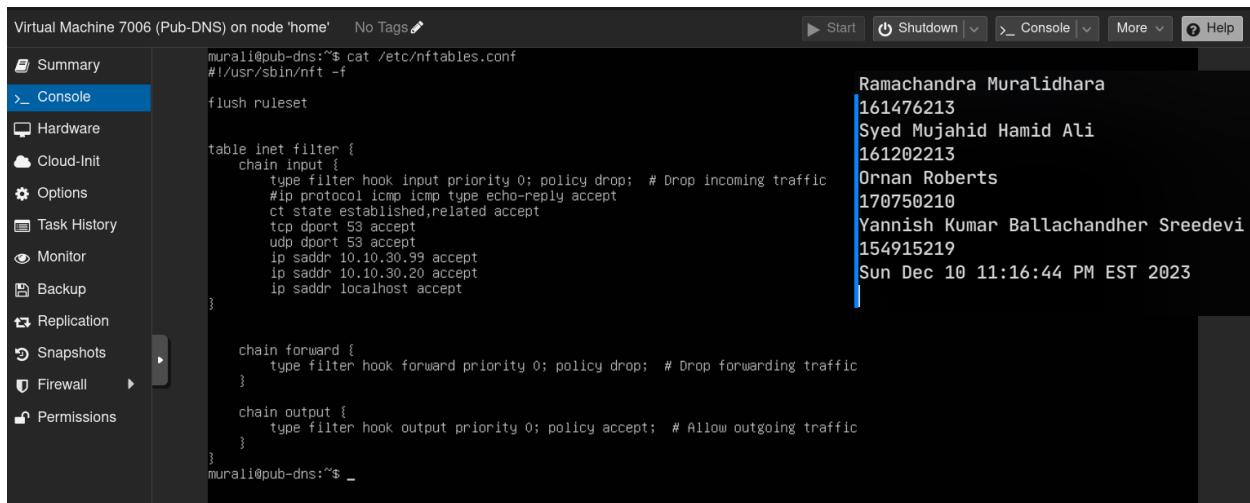
    chain forward {
        type filter hook forward priority 0; policy drop; # Drop forwarding traffic
    }

    chain output {
        type filter hook output priority 0; policy accept; # Allow outgoing traffic
    }
}

murali@priv-dns:/etc/bind/zones$
```

Ramachandra Muralidhara
161476213
Syed Mujahid Hamid Ali
161202213
Ornan Roberts
170750210
Yannish Kumar Ballachandher Sreedevi
154915219
Sun Dec 10 11:15:20 PM EST 2023

Public DNS



This screenshot is similar to the previous one, showing the Oracle VM VirtualBox Manager interface with the 'Firewall' setting selected. The terminal window shows the same `cat /etc/nftables.conf` command and its output. The configuration is identical to the Private DNS host, with rules for the 'filter' table's 'inet' chain. A list of names and their corresponding IDs is also present on the right.

```
murali@pub-dns:~$ cat /etc/nftables.conf
#!/usr/sbin/nft -f

flush ruleset

table inet filter {
    chain input {
        type filter hook input priority 0; policy drop; # Drop incoming traffic
        ip protocol icmp icmp type echo-reply accept
        ct state established,related accept
        tcp dport 53 accept
        udp dport 53 accept
        ip saddr 10.10.30.99 accept
        ip saddr 10.10.30.20 accept
        ip saddr localhost accept
    }

    chain forward {
        type filter hook forward priority 0; policy drop; # Drop forwarding traffic
    }

    chain output {
        type filter hook output priority 0; policy accept; # Allow outgoing traffic
    }
}

murali@pub-dns:~$
```

Ramachandra Muralidhara
161476213
Syed Mujahid Hamid Ali
161202213
Ornan Roberts
170750210
Yannish Kumar Ballachandher Sreedevi
154915219
Sun Dec 10 11:16:44 PM EST 2023

Private Containers Host

Virtual Machine 7009 (Priv-Containers-Host) on node 'home' No Tags

Start Shutdown Console More Help

Summary Console Hardware Cloud-Init Options Task History Monitor Backup Replication Snapshots Firewall Permissions

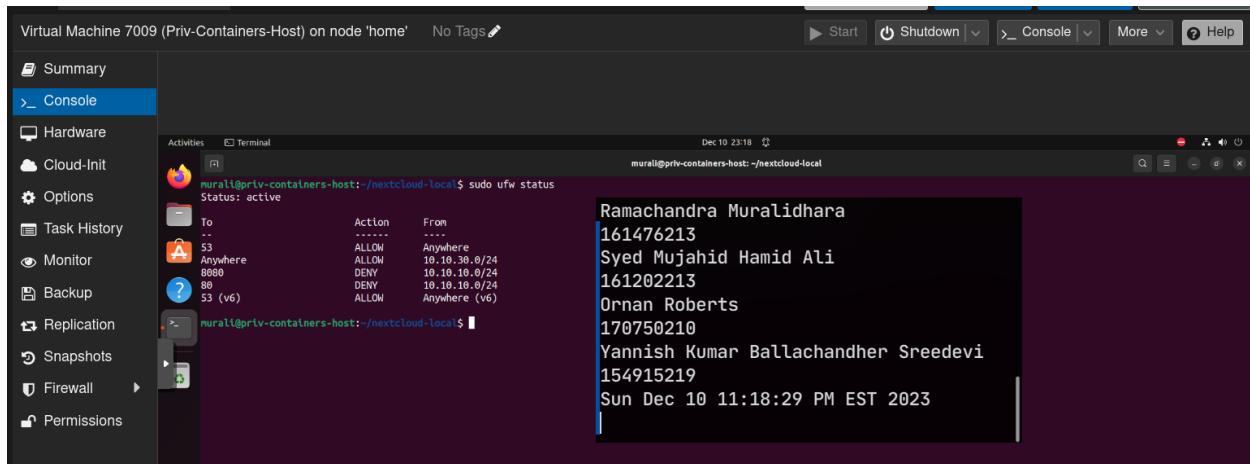
Activities Terminal

murali@priv-containers-host:~/nextcloud-local\$ sudo ufw status

To	Action	From
...	ALLOW	Anywhere
53	ALLOW	10.10.30.0/24
Anywhere	ALLOW	10.10.10.0/24
8080	DENY	10.10.10.0/24
80	DENY	10.10.10.0/24
53 (v6)	ALLOW	Anywhere (v6)

murali@priv-containers-host:~/nextcloud-local\$

Ramachandra Muralidhara
161476213
Syed Mujahid Hamid Ali
161202213
Ornan Roberts
170750210
Yannish Kumar Ballachandher Sreedevi
154915219
Sun Dec 10 11:18:29 PM EST 2023



Public Containers Host

Virtual Machine 7010 (Pub-Containers-Host) on node 'home' No Tags

Start Shutdown Console More Help

Summary Console Hardware Cloud-Init Options Task History Monitor Backup Replication Snapshots Firewall Permissions

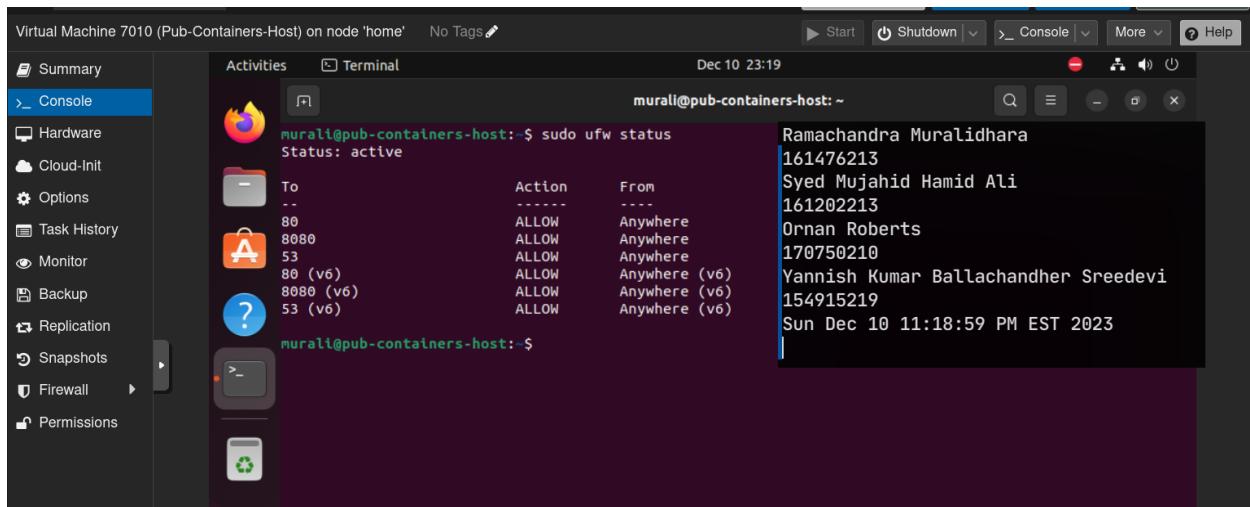
Activities Terminal

murali@pub-containers-host:~\$ sudo ufw status

To	Action	From
--	-----	-----
80	ALLOW	Anywhere
8080	ALLOW	Anywhere
53	ALLOW	Anywhere
80 (v6)	ALLOW	Anywhere (v6)
8080 (v6)	ALLOW	Anywhere (v6)
53 (v6)	ALLOW	Anywhere (v6)

murali@pub-containers-host:~\$

Ramachandra Muralidhara
161476213
Syed Mujahid Hamid Ali
161202213
Ornan Roberts
170750210
Yannish Kumar Ballachandher Sreedevi
154915219
Sun Dec 10 11:18:59 PM EST 2023



VPN Configuration

The following is the VPN configurations that were added for client and server side. The tunnel configuration can be seen below.

Server Configuration File

```
GNU nano 6.2
-----END DH PARAMETERS----- > /etc/openvpn/server/dh.pem
# Generate server.conf
cp etc/local $in

port $port
proto $protocol
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
auth SHA512
tls-crypt tc.key
topology subnet
server "10.8.0.0 255.255.255.0" > /etc/openvpn/server/server.conf
        if [[ -z "$sips" ]]; then
            echo 'push "redirect-gateway def1 bypass-dhcp"' >> /etc/openvpn/server/server.conf
        else
            echo 'server-ipv4 fddd:194:1194::/64' >> /etc/openvpn/server/server.conf
            echo 'push "redirect-gateway def1 ipv6 bypass-dhcp"' >> /etc/openvpn/server/server.conf
        fi
        echo 'ifconfig-pool-persist ip.txt' >> /etc/openvpn/server/server.conf
# DNS
case "$sdns" in
    1|""") # Locate the proper resolv.conf
        # Needed for systems running systemd-resolved
        if grep '^nameserver' "/etc/resolv.conf" | grep -qv '127.0.0.53' ; then
            resolv_conf="/etc/resolv.conf"
        else
            resolv_conf="/run/systemd/resolve/resolv.conf"
        fi
        # Obtain the resolvers from resolv.conf and use them for OpenVPN
        grep -v '#'; "$resolv_conf" | grep 'nameserver' | grep -v '127.0.0.53' | grep -oE '[0-9]{1,3}(\.[0-9]{1,3}){3}' >> /etc/openvpn/server/server.conf
done
;;
2)
echo 'push "dhcp-option DNS 8.8.8.8"' >> /etc/openvpn/server/server.conf
echo 'push "dhcp-option DNS 8.8.4.4"' >> /etc/openvpn/server/server.conf
;;
3)
echo 'push "dhcp-option DNS 1.1.1.1"' >> /etc/openvpn/server/server.conf
echo 'push "dhcp-option DNS 1.0.0.1"' >> /etc/openvpn/server/server.conf
```

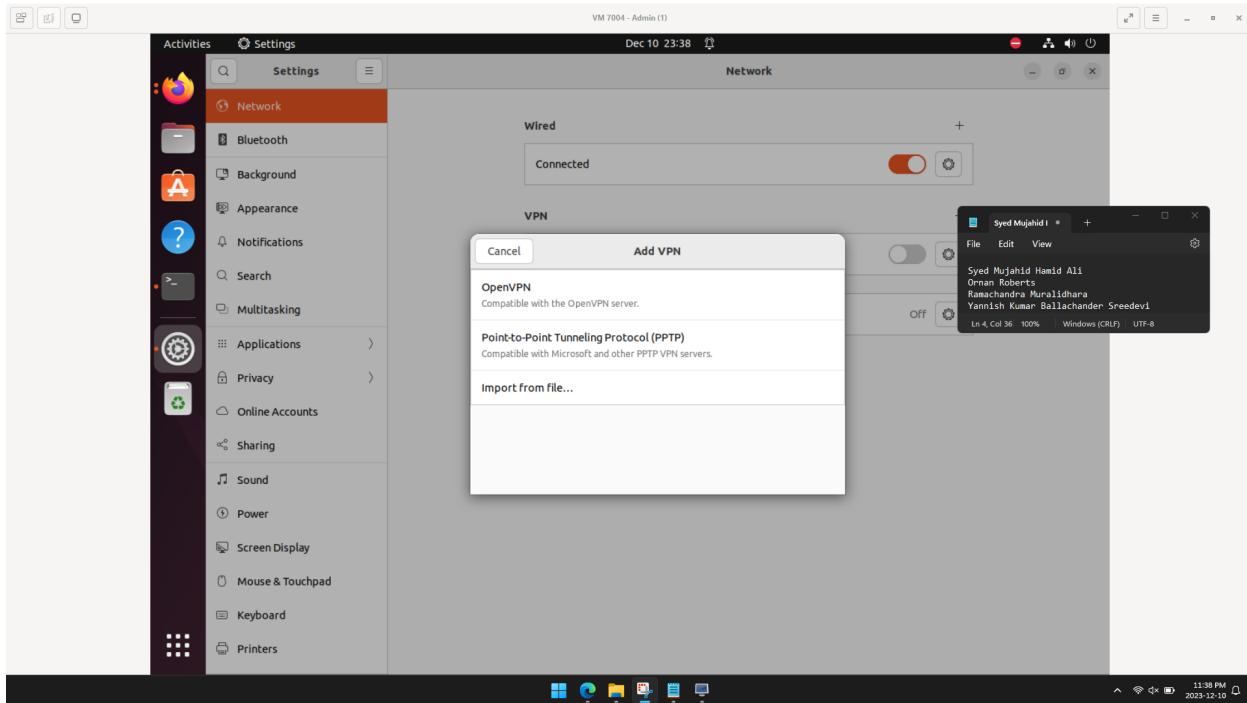
Client Configuration File

```
GNU nano 6.2                                admin owned

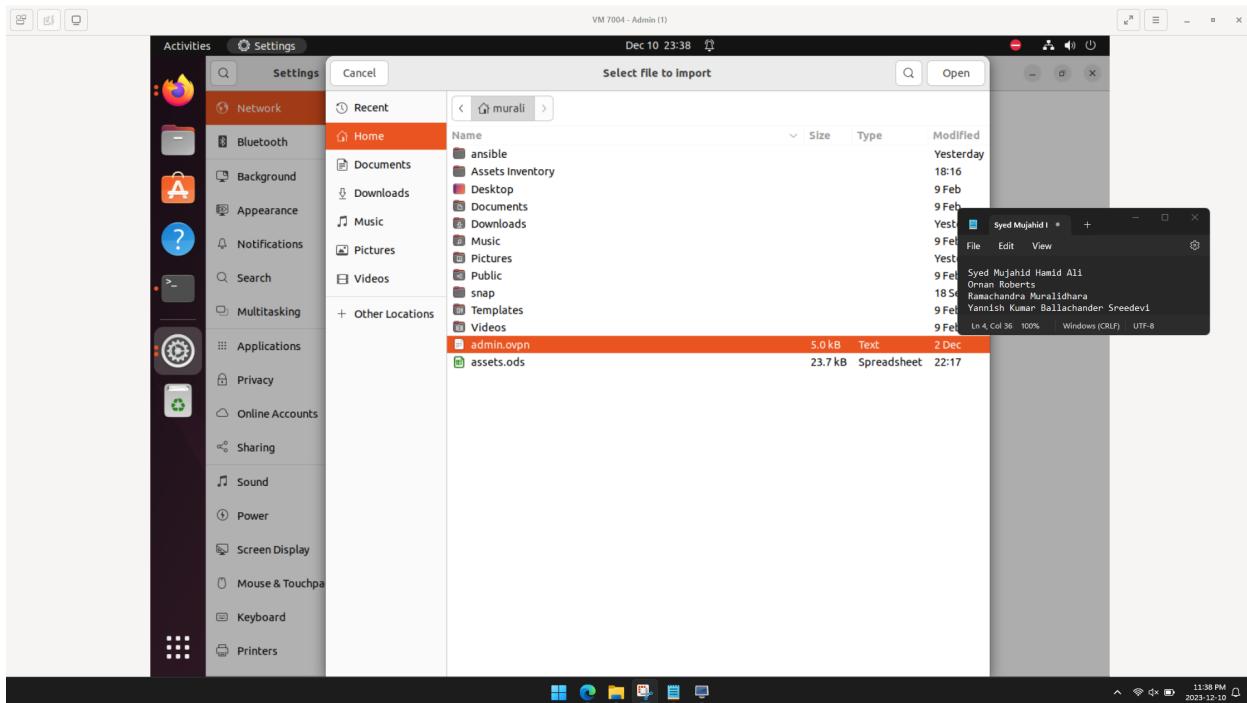
client
dev tun
dev udp
remote 10.10.10.20 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA512
ignore-unknown-option block-outside-dns
verb 3
ca

-----BEGIN CERTIFICATE-----
MIIDUzCAJ0gAwIBRQIjpuFwdwqjBe2J57EzWHunVluDQYJk02IhvcNAQEL
BQHJMjEJUMBGA1UEAww1S3U0EgQ0EuHnCNJMMkjyHjyHjuJaZkhcnNM2X
MT15MjAuNjAzKwMAMQRQgEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
AQEBBQDgEgPDCCAQ0gEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
S34mBiacLn78bd0tn7k3rKLFLNCKmgIzTr56WkmFka2r7VfWaDpmf+upLko
8FX3bJrxs9Yf1jchta25TpkyPRMVGHWXB5BE5dd/b/H2GVMpkHZvXUKC
H1V/1Sp5TDCvcvccu20J10d0H2zKQfTtuH87zKDSmH16Ypnm0tg1vqloGh5RL
t5vEy1lQ1R7Mlls05ggEf0ng04cgxvIC18nXh5205pmrh8xB5j-R
Hu/vwsG771brL8npGhCeHNTsa0dQpxg9QSSf5ChwAra0BkDCBjTRM
BgHvMRMEBA0TADQH-MB05B10d0gQHBSJ1eSgEf1fruxxtBwcaKs*x+fJndTBRBgN
HSMEsJB1g0ESEf1fruxxtBwcaKs*x+fJndTBRBgN
-----END CERTIFICATE-----
</ca>
<cert>
-----BEGIN CERTIFICATE-----
MIIDUzCAJ0gAwIBRQIjpuFwdwqjBe2J57EzWHunVluDQYJk02IhvcNAQEL
BQHJMjEJUMBGA1UEAww1S3U0EgQ0EuHnCNJMMkjyHjyHjuJaZkhcnNM2X
MT15MjAuNjAzKwMAMQRQgEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
AQEBBQDgEgPDCCAQ0gEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
S34mBiacLn78bd0tn7k3rKLFLNCKmgIzTr56WkmFka2r7VfWaDpmf+upLko
8FX3bJrxs9Yf1jchta25TpkyPRMVGHWXB5BE5dd/b/H2GVMpkHZvXUKC
H1V/1Sp5TDCvcvccu20J10d0H2zKQfTtuH87zKDSmH16Ypnm0tg1vqloGh5RL
t5vEy1lQ1R7Mlls05ggEf0ng04cgxvIC18nXh5205pmrh8xB5j-R
Hu/vwsG771brL8npGhCeHNTsa0dQpxg9QSSf5ChwAra0BkDCBjTRM
BgHvMRMEBA0TADQH-MB05B10d0gQHBSJ1eSgEf1fruxxtBwcaKs*x+fJndTBRBgN
HSMEsJB1g0ESEf1fruxxtBwcaKs*x+fJndTBRBgN
-----END CERTIFICATE-----
</cert>
-----BEGIN CERTIFICATE-----
MIIDUzCAJ0gAwIBRQIjpuFwdwqjBe2J57EzWHunVluDQYJk02IhvcNAQEL
BQHJMjEJUMBGA1UEAww1S3U0EgQ0EuHnCNJMMkjyHjyHjuJaZkhcnNM2X
MT15MjAuNjAzKwMAMQRQgEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
AQEBBQDgEgPDCCAQ0gEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
S34mBiacLn78bd0tn7k3rKLFLNCKmgIzTr56WkmFka2r7VfWaDpmf+upLko
8FX3bJrxs9Yf1jchta25TpkyPRMVGHWXB5BE5dd/b/H2GVMpkHZvXUKC
H1V/1Sp5TDCvcvccu20J10d0H2zKQfTtuH87zKDSmH16Ypnm0tg1vqloGh5RL
t5vEy1lQ1R7Mlls05ggEf0ng04cgxvIC18nXh5205pmrh8xB5j-R
Hu/vwsG771brL8npGhCeHNTsa0dQpxg9QSSf5ChwAra0BkDCBjTRM
BgHvMRMEBA0TADQH-MB05B10d0gQHBSJ1eSgEf1fruxxtBwcaKs*x+fJndTBRBgN
HSMEsJB1g0ESEf1fruxxtBwcaKs*x+fJndTBRBgN
-----END CERTIFICATE-----
</cert>
-----BEGIN CERTIFICATE-----
MIIDUzCAJ0gAwIBRQIjpuFwdwqjBe2J57EzWHunVluDQYJk02IhvcNAQEL
BQHJMjEJUMBGA1UEAww1S3U0EgQ0EuHnCNJMMkjyHjyHjuJaZkhcnNM2X
MT15MjAuNjAzKwMAMQRQgEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
AQEBBQDgEgPDCCAQ0gEYDwQ0DdATfYXN5LVTTQSBDQTCAStuQVJk0zIhvcN
S34mBiacLn78bd0tn7k3rKLFLNCKmgIzTr56WkmFka2r7VfWaDpmf+upLko
8FX3bJrxs9Yf1jchta25TpkyPRMVGHWXB5BE5dd/b/H2GVMpkHZvXUKC
H1V/1Sp5TDCvcvccu20J10d0H2zKQfTtuH87zKDSmH16Ypnm0tg1vqloGh5RL
t5vEy1lQ1R7Mlls05ggEf0ng04cgxvIC18nXh5205pmrh8xB5j-R
Hu/vwsG771brL8npGhCeHNTsa0dQpxg9QSSf5ChwAra0BkDCBjTRM
BgHvMRMEBA0TADQH-MB05B10d0gQHBSJ1eSgEf1fruxxtBwcaKs*x+fJndTBRBgN
HSMEsJB1g0ESEf1fruxxtBwcaKs*x+fJndTBRBgN
-----END CERTIFICATE-----
</cert>
```

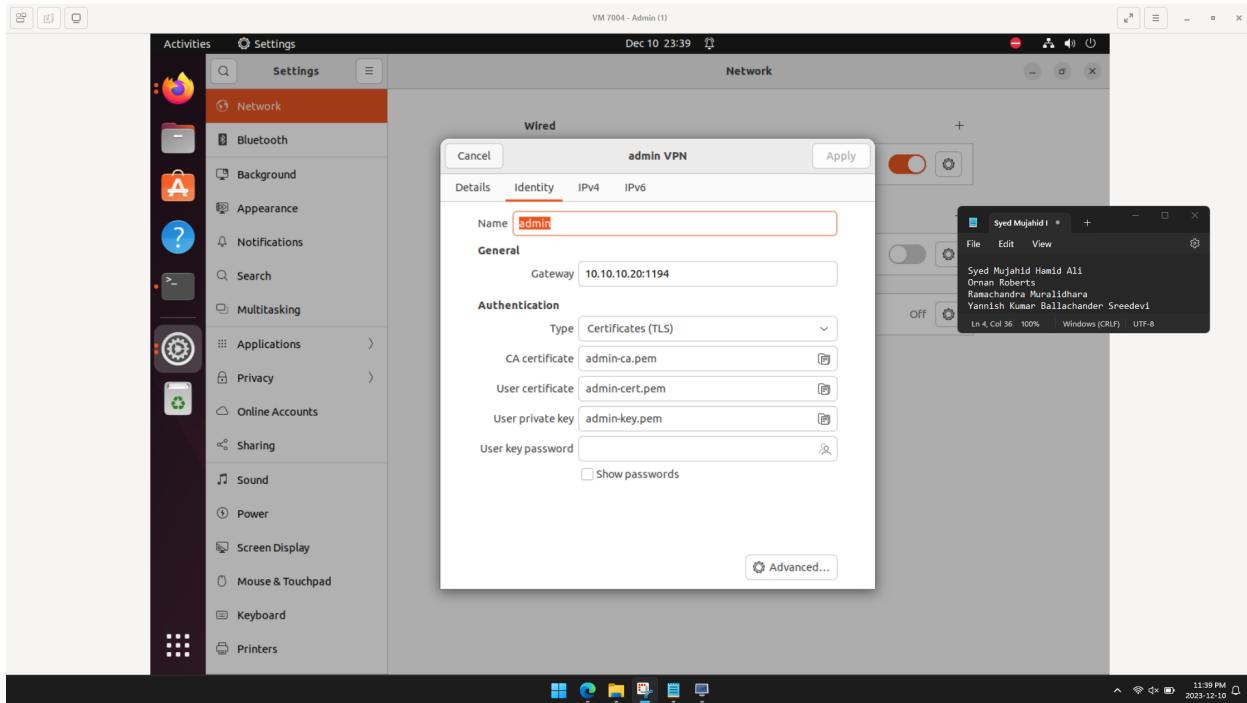
Using Ubuntu UI to add VPN Configuration File on the Client



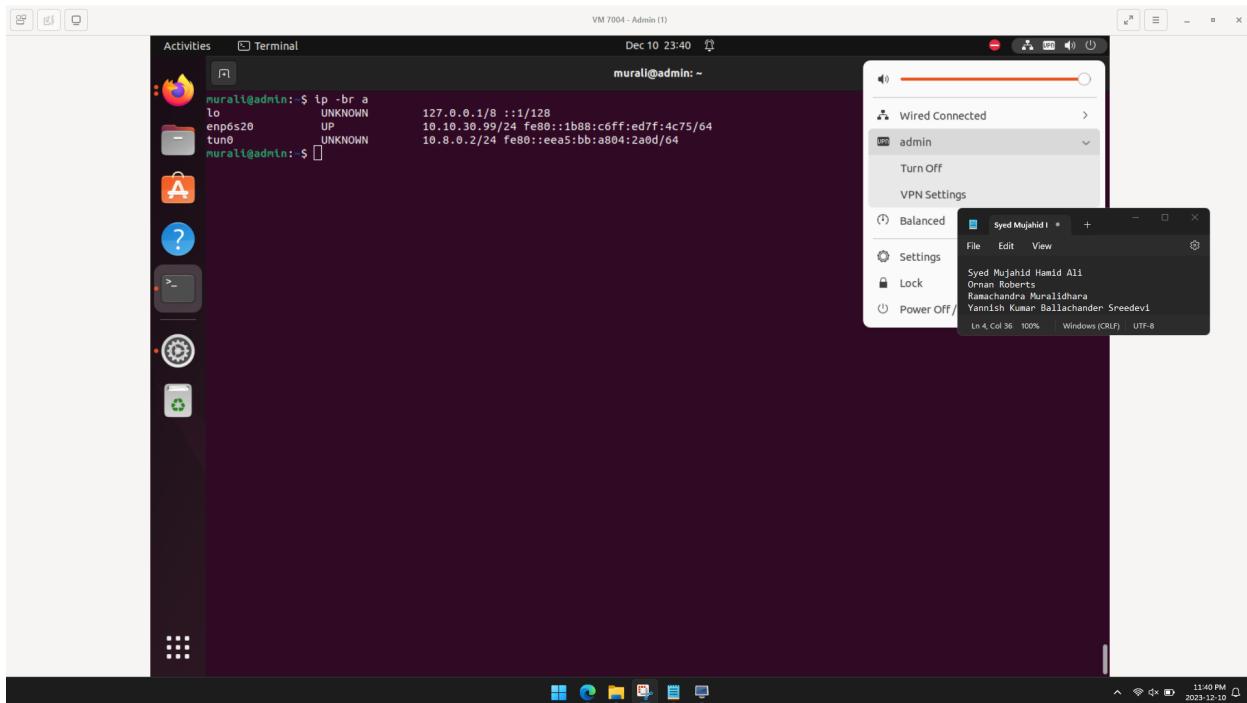
Selecting the Configuration File



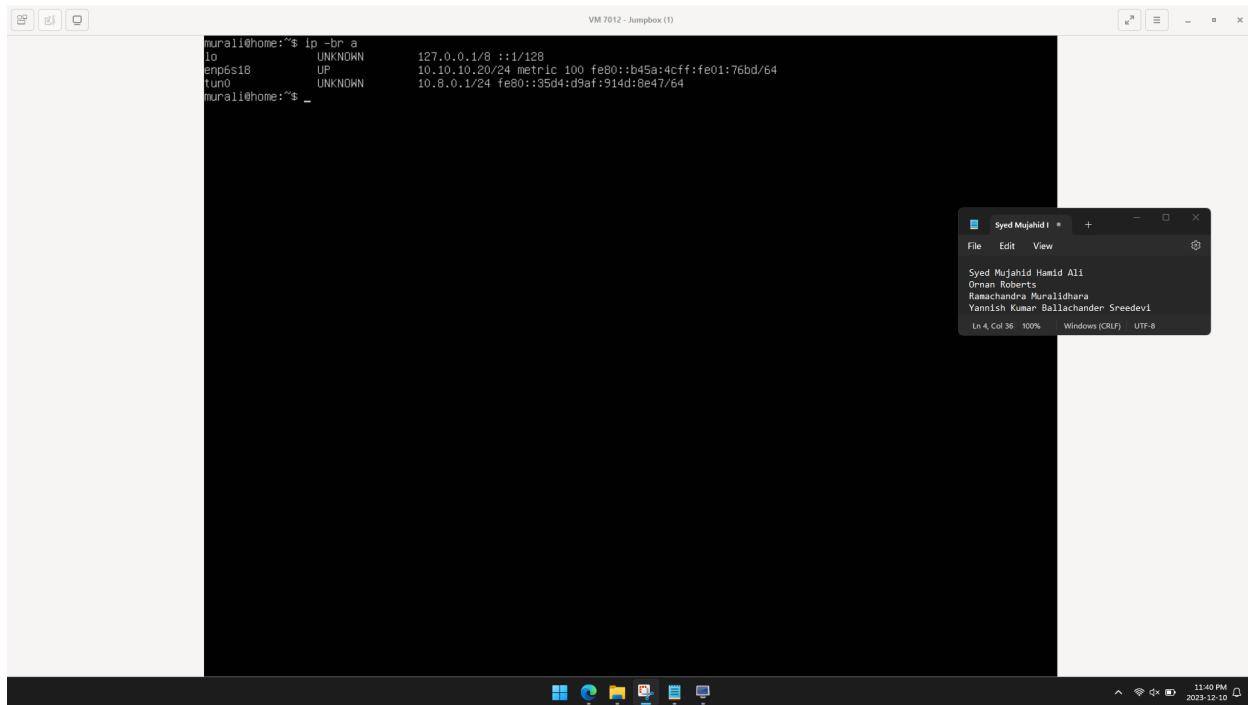
Adding the right certificates and other files



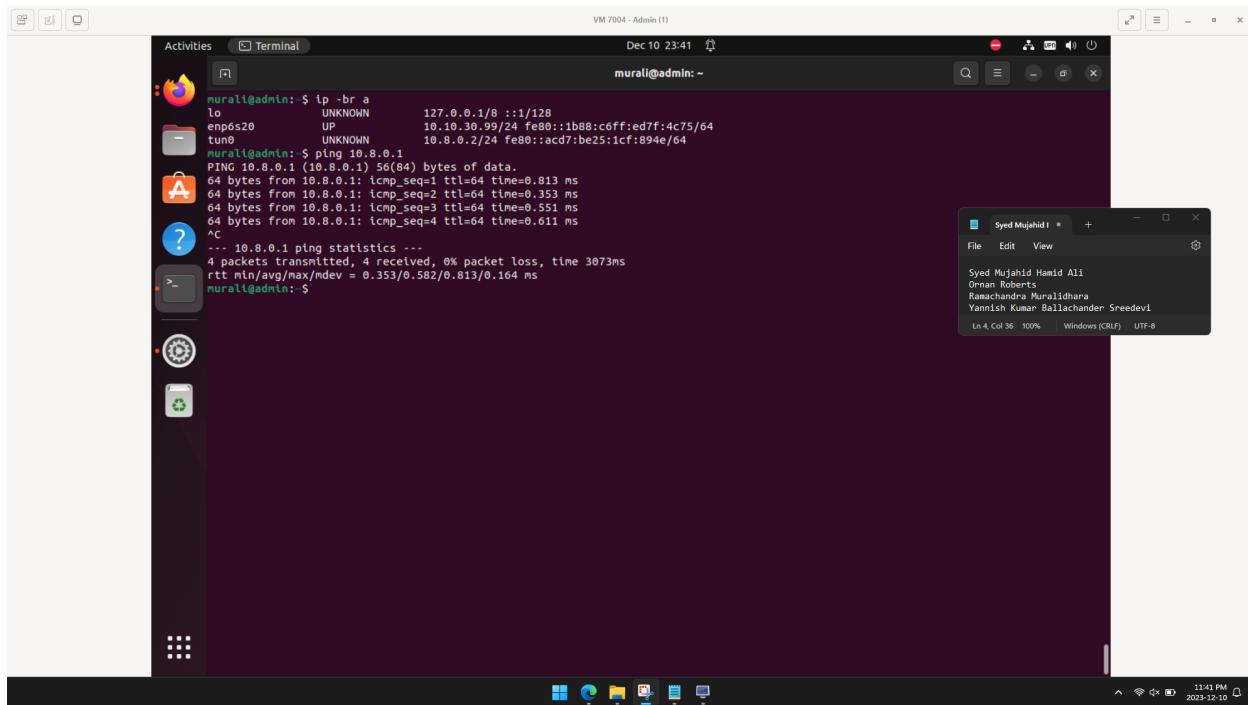
Tunnel interface created on Client when VPN is turned on



Tunnel interface on the Server



Successful ping attempt made from Client to Server



Conclusion

In conclusion, this report showcased the low-level design and functional testing in comprehensive overview manners of the Agricore infrastructure. Based on the designed business requirements of an e-commerce platform we were able to demonstrate the system design, security implementation, and functional testing. The business requirements are translated into a robust infrastructure design. The system design incorporated a zone segmentation model. The model was designed with distinct security controls. Controls were implemented to safeguard information, systems, and assets. The functional testing demonstrated a commitment to meeting business requirements. The report reflects a well-executed low-level implementation and design, emphasizing security, functionality, and adherence to business requirements.