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

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 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.

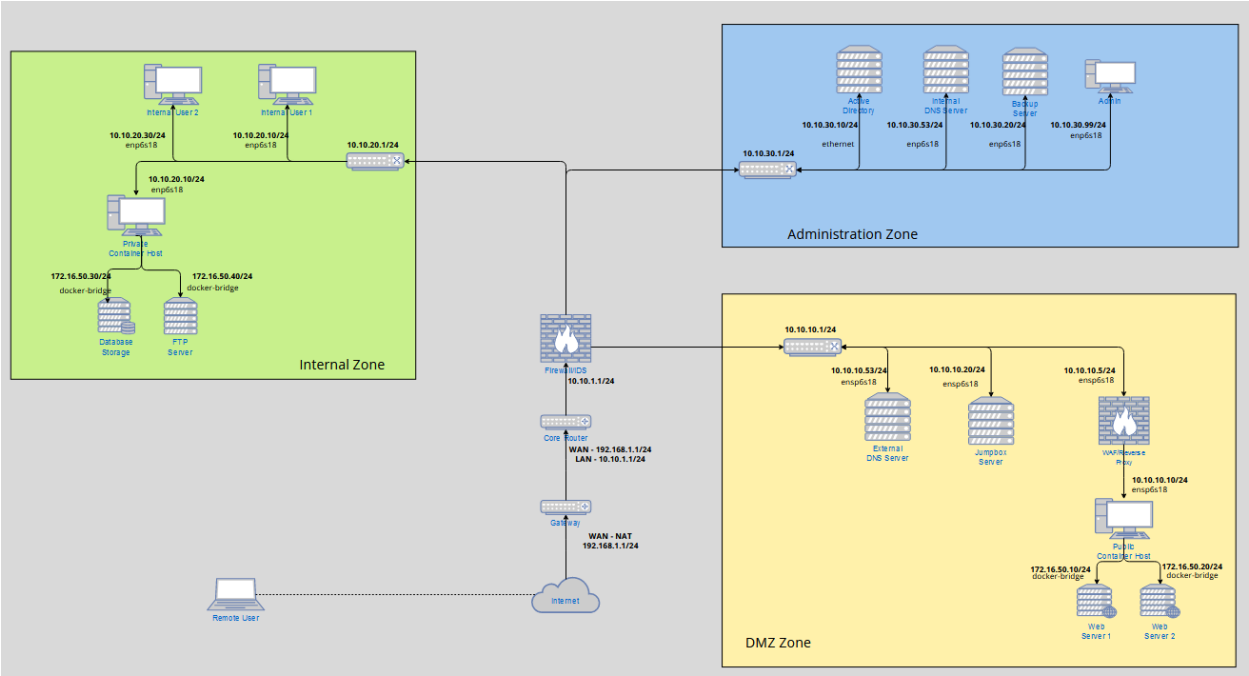


Fig.1 Network Design with zones segmentation

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.

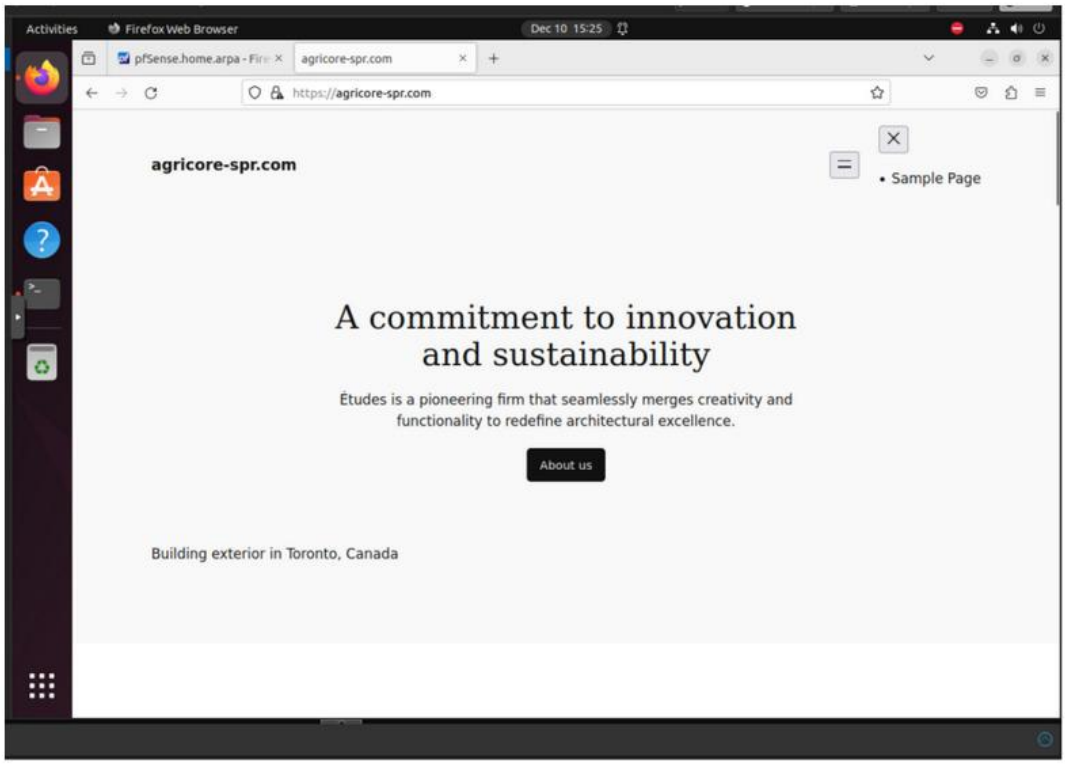
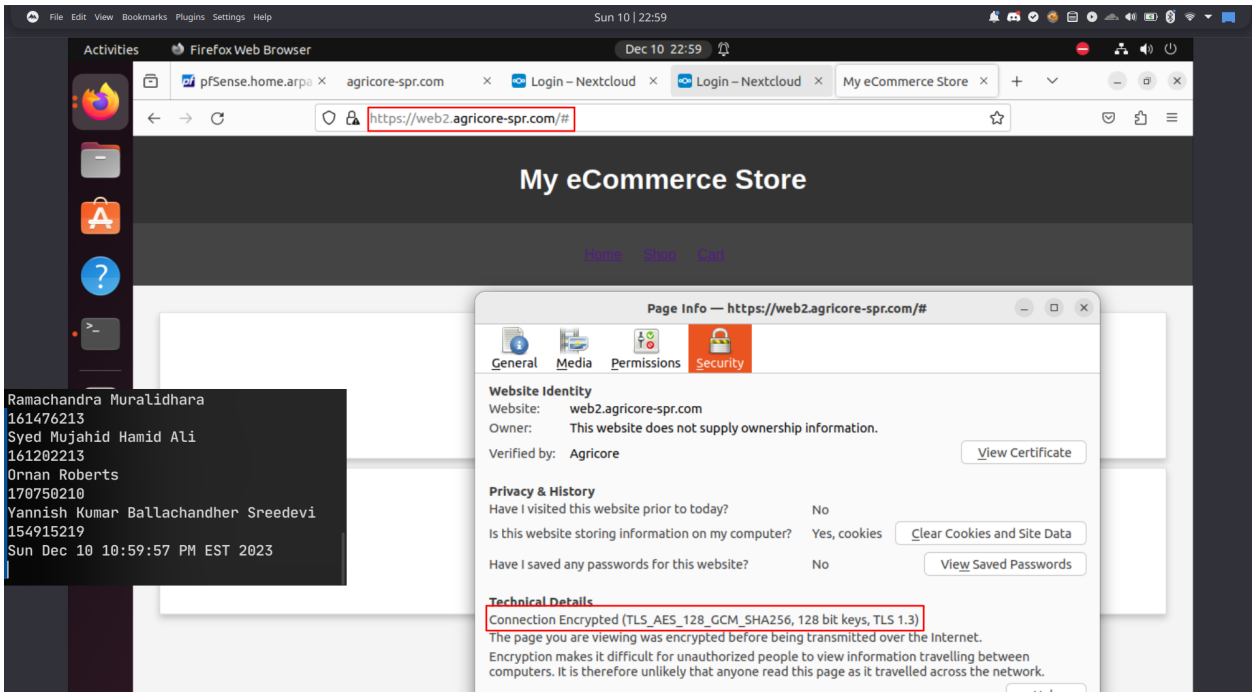
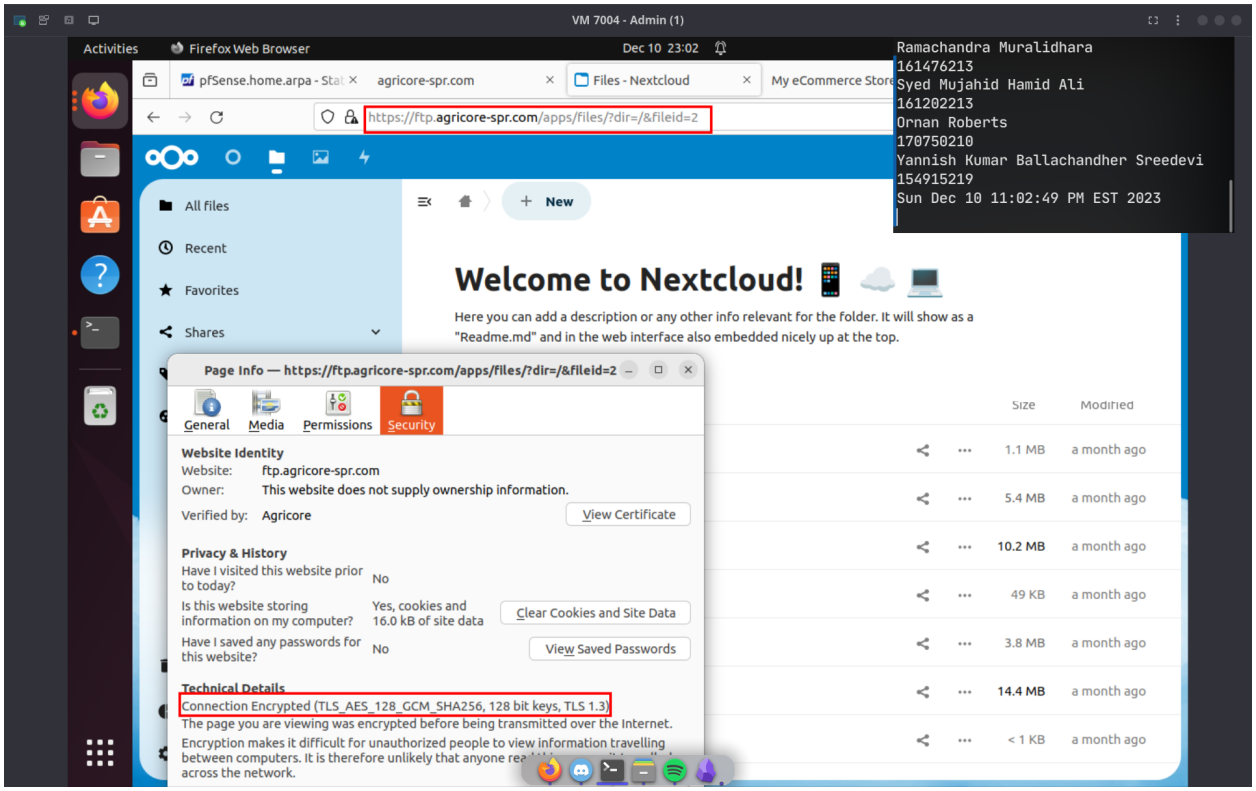


Fig.13 SSL certificate added and site with https

E-Commerce

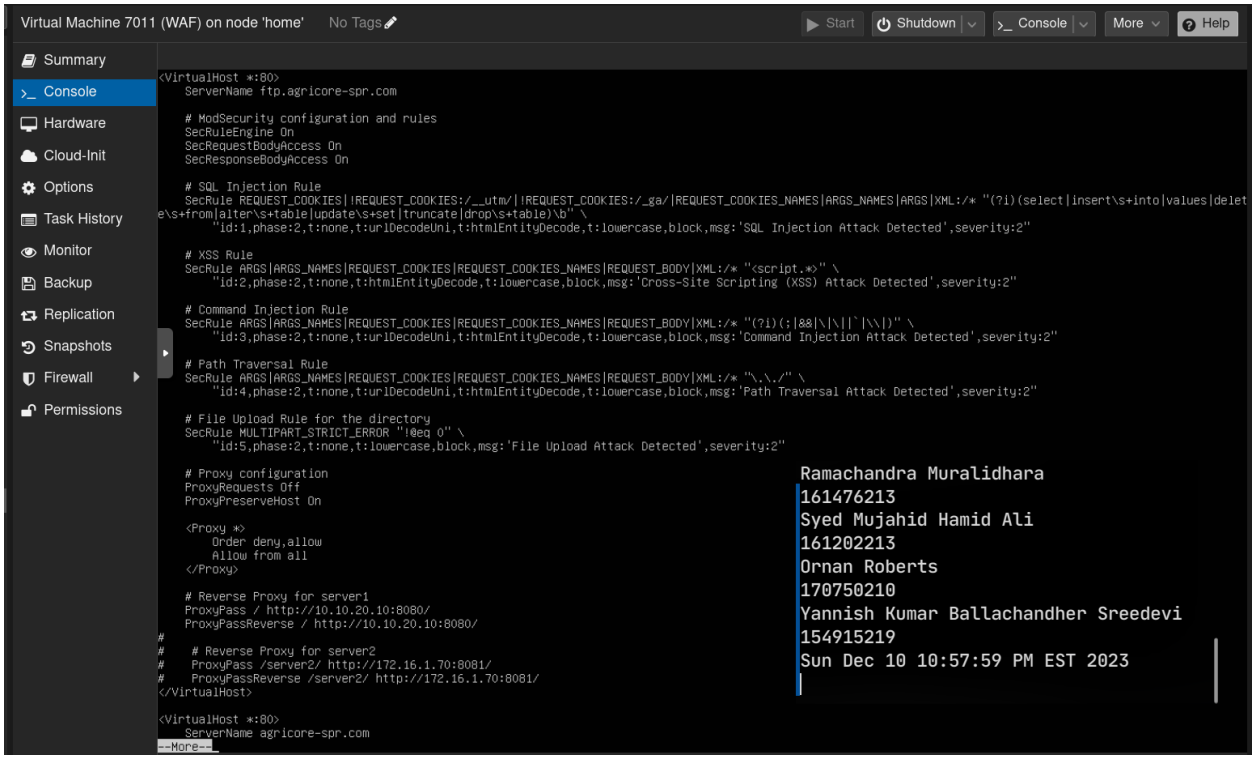


Secured Website (FTP/Nextcloud)



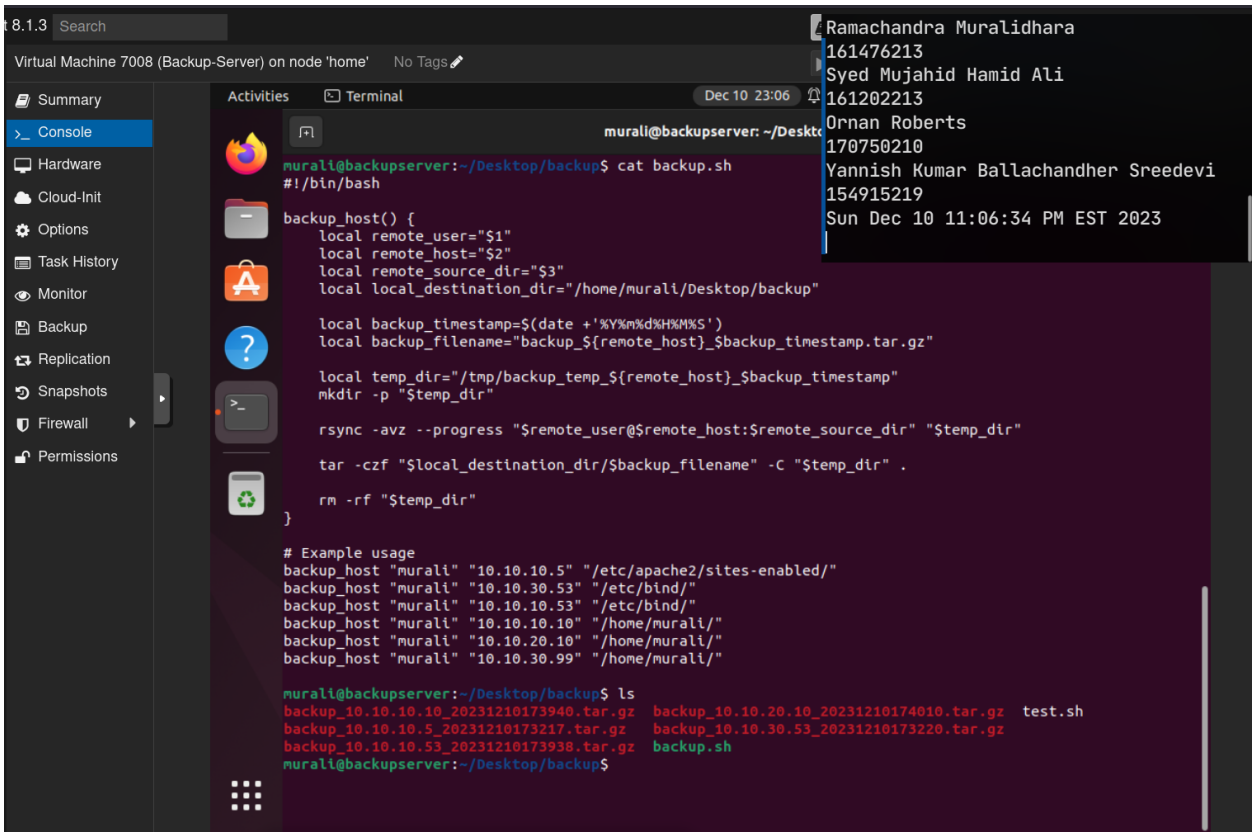
Web Application Firewall

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.



Backup Script

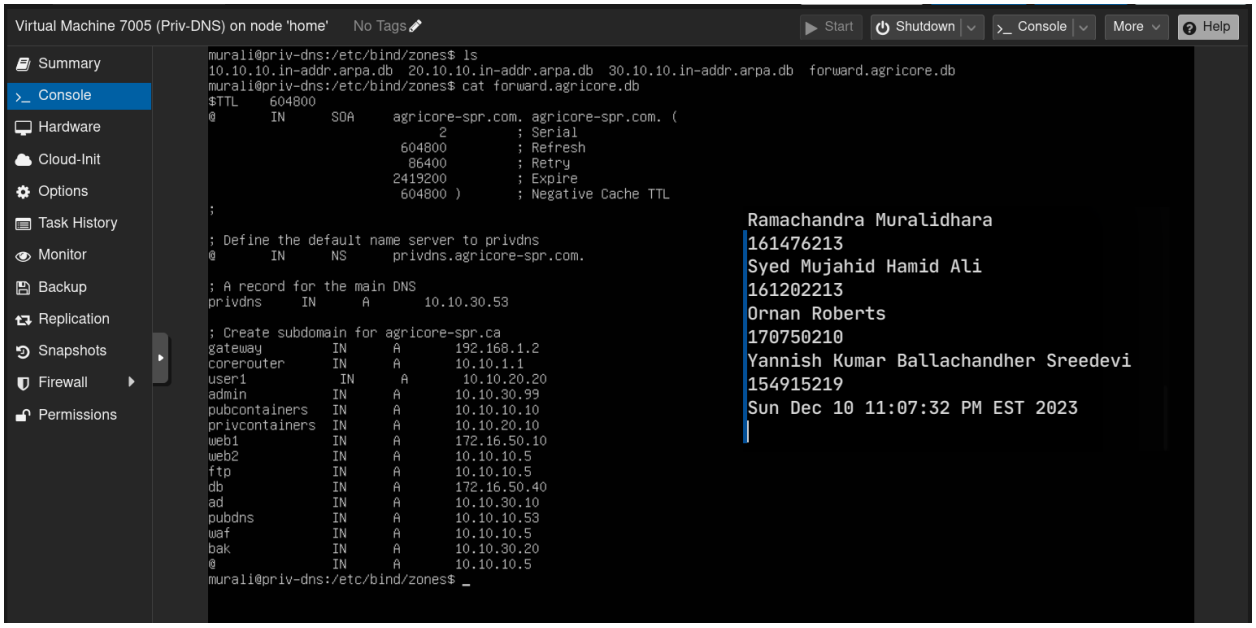
The backup plan was initiated using a script which backup configurations using rsync. The script is designed to save files onto local admin pc.



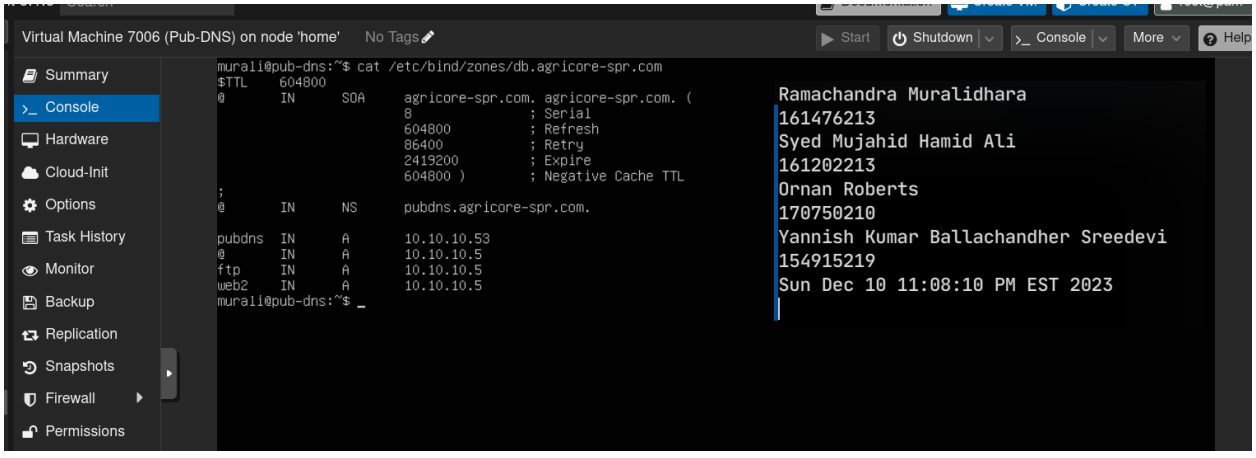
DNS

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



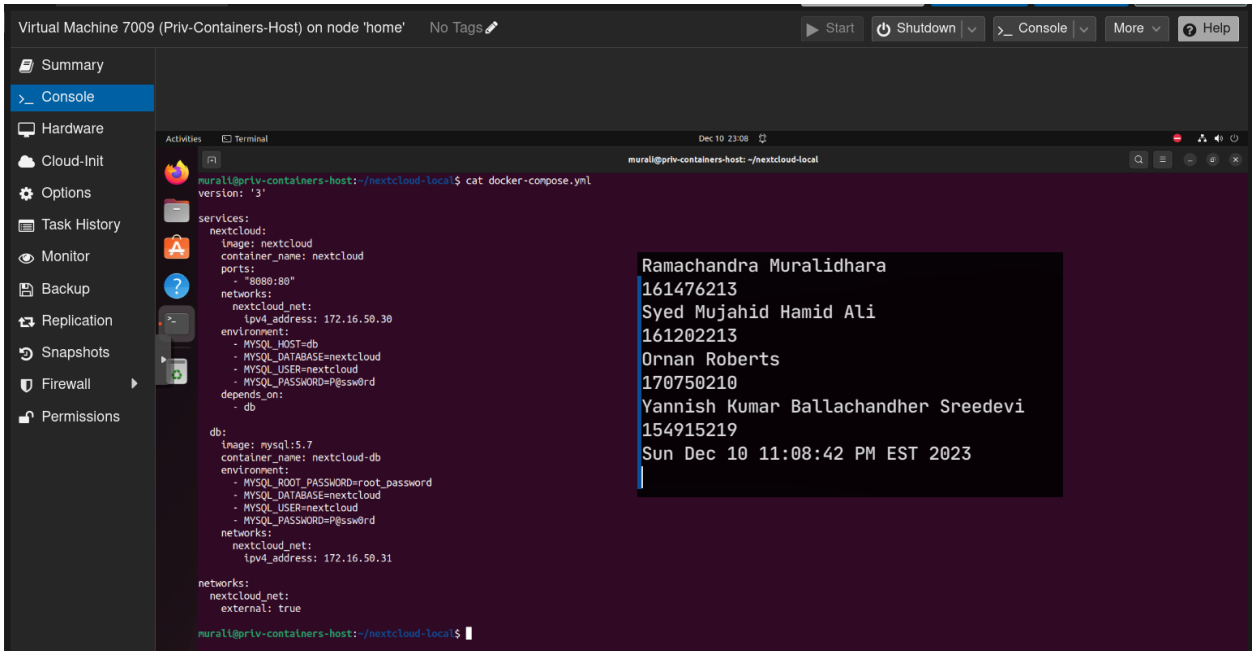
Public DNS



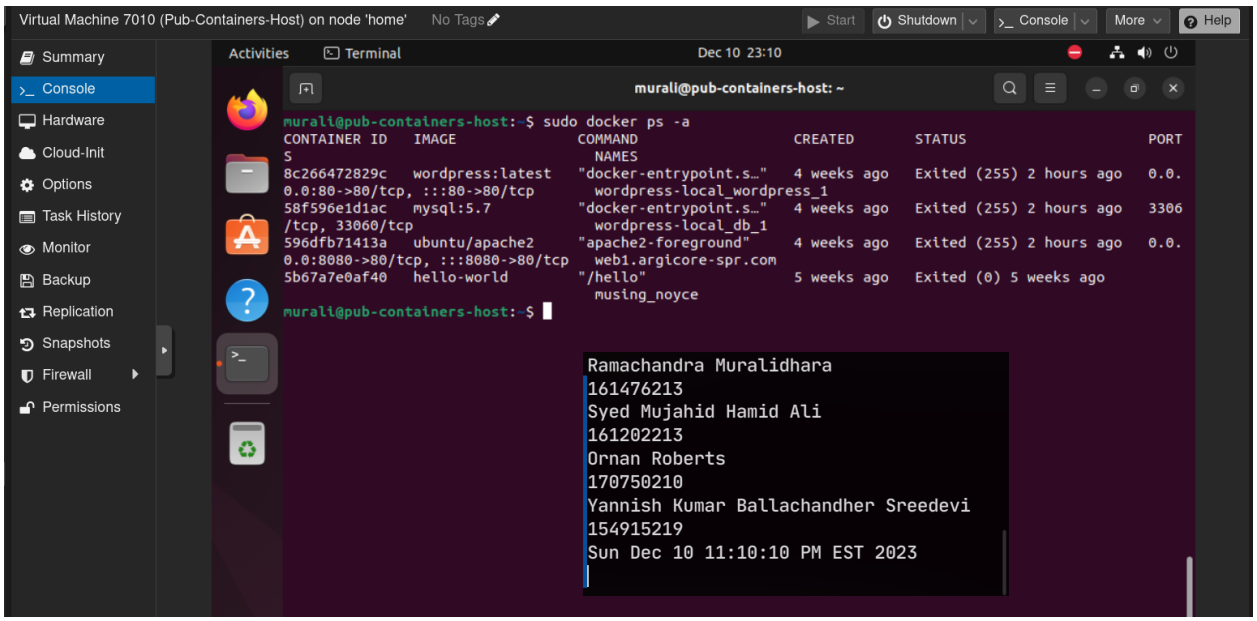
Database

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



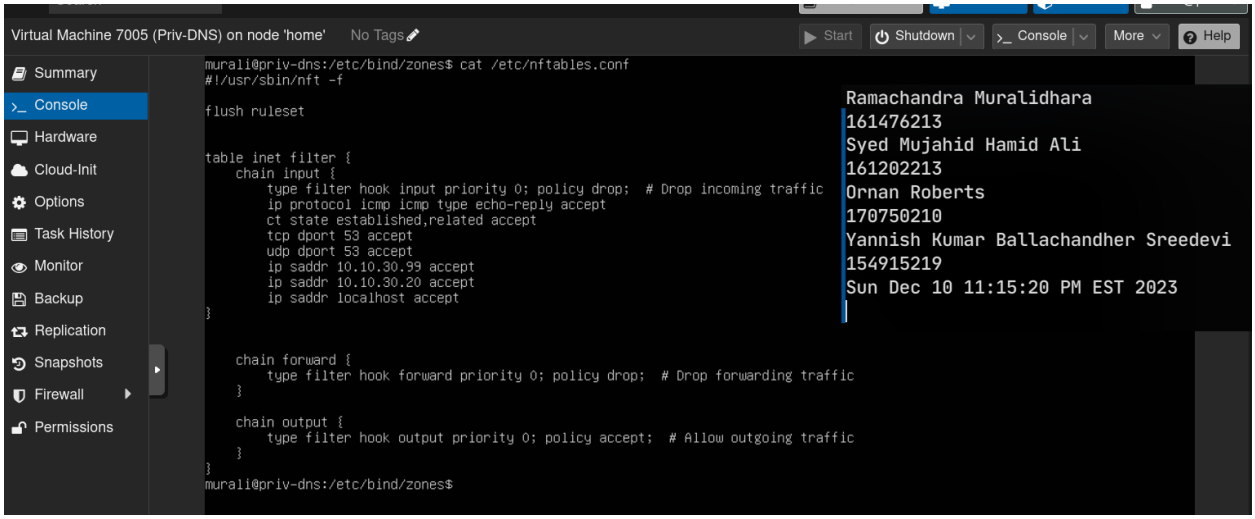
Web Servers



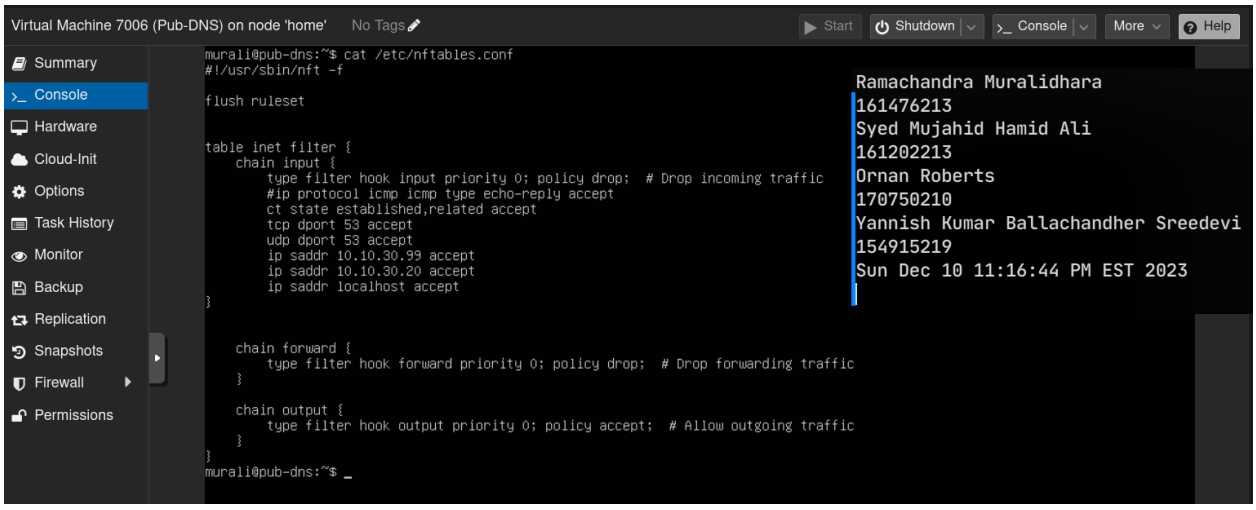
Firewall configurations

Host Based

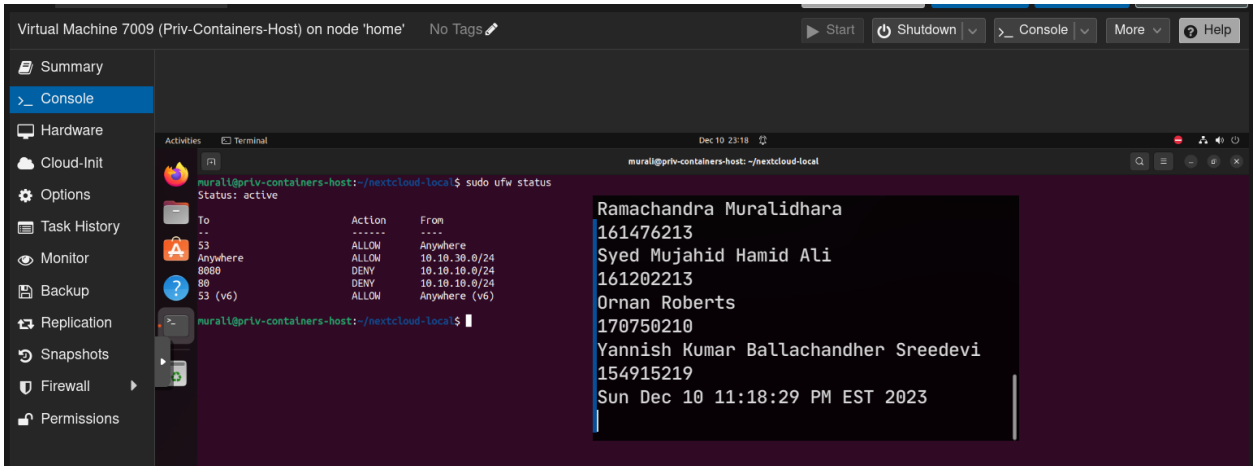
Private DNS



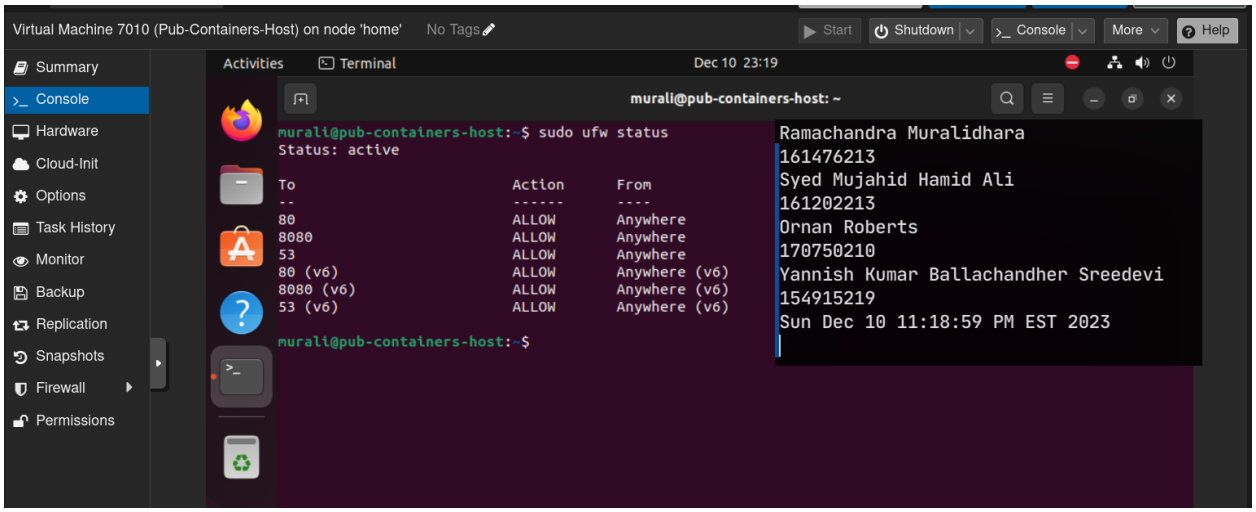
Public DNS



Private Containers Host



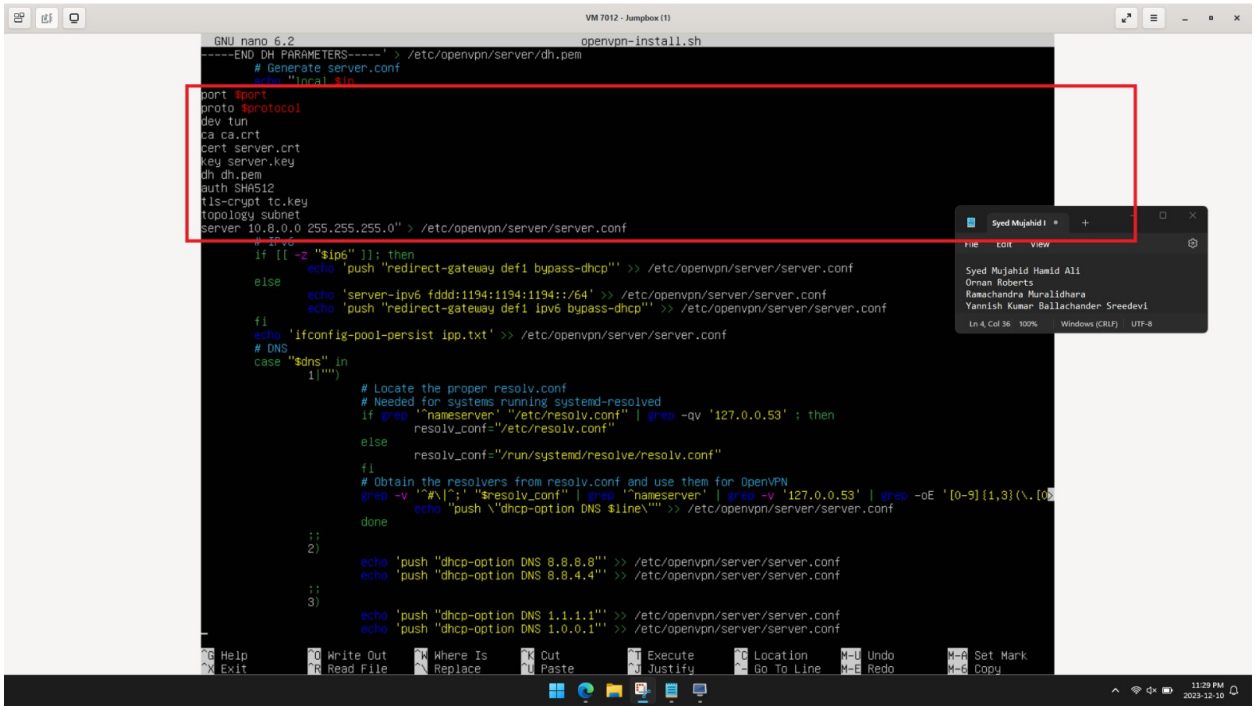
Public Containers Host



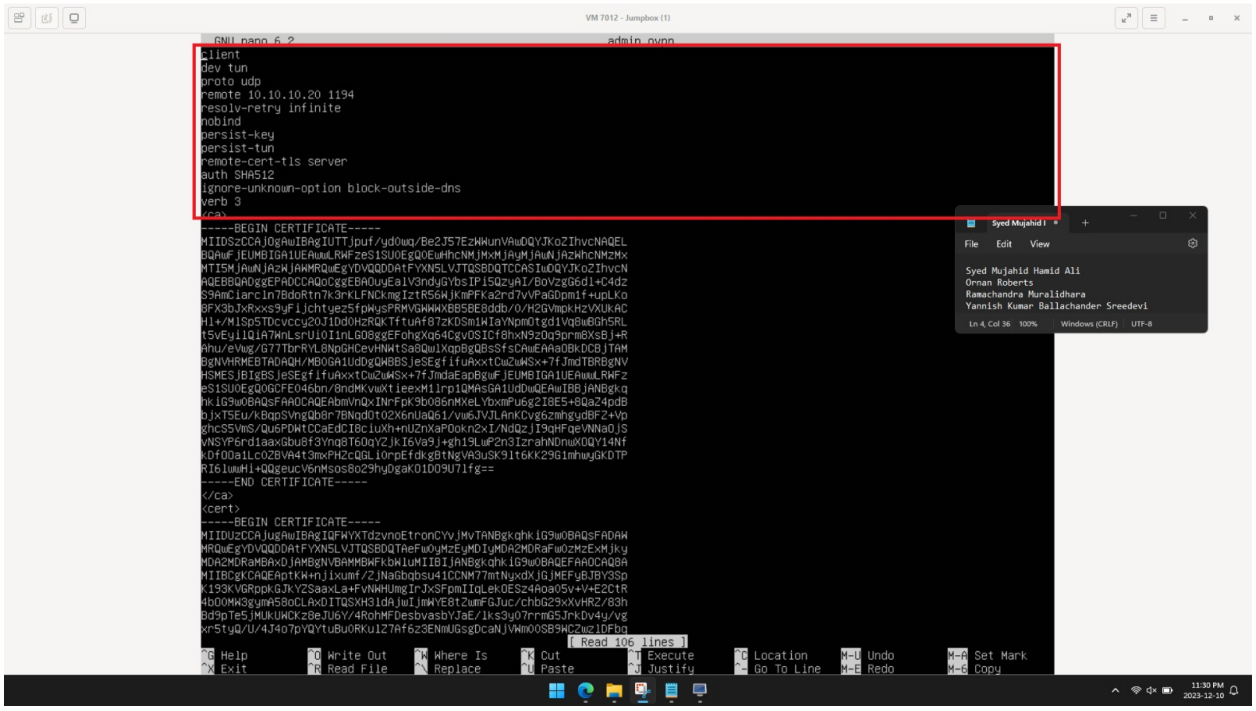
VPN Configuration

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

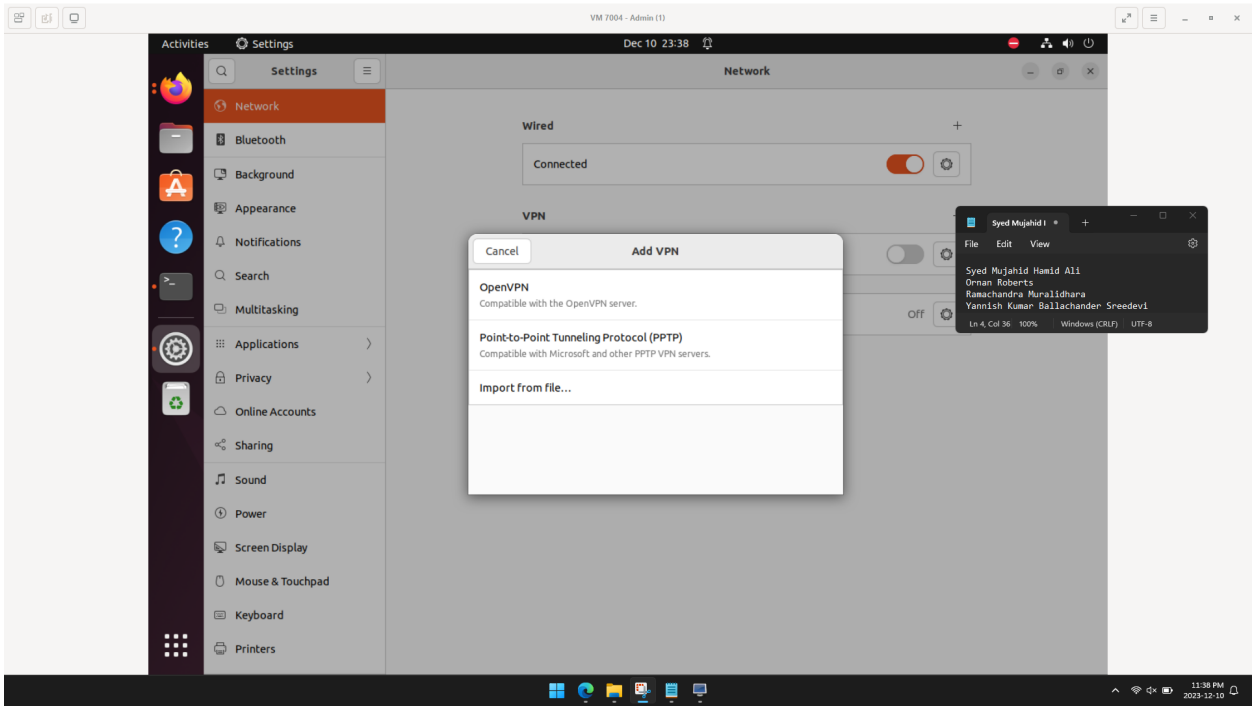
Server Configuration File



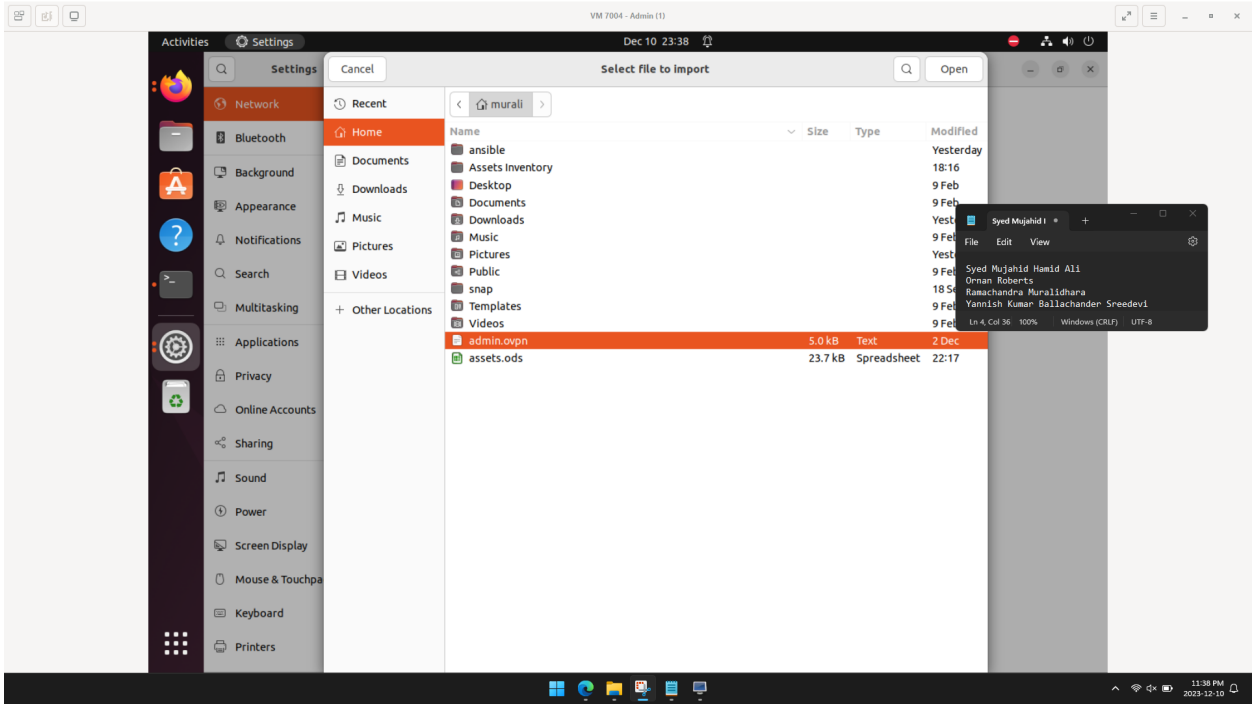
Client Configuration File



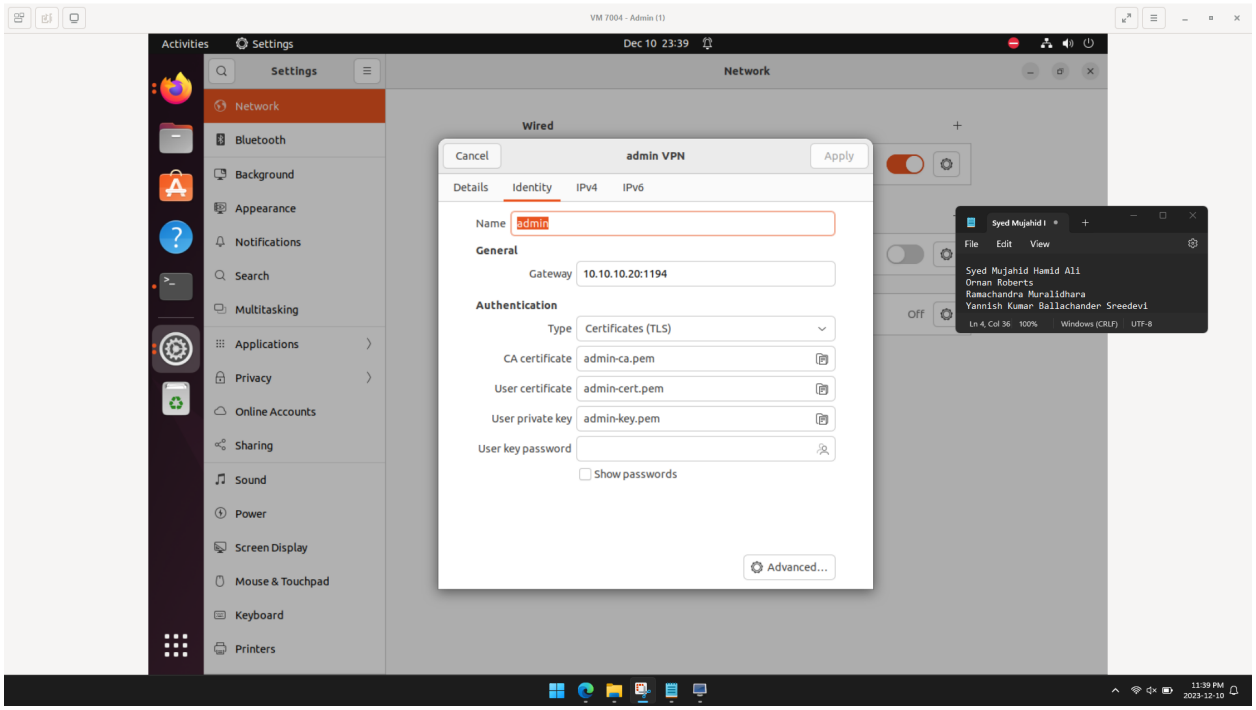
Using Ubuntu UI to add VPN Configuration File on the Client



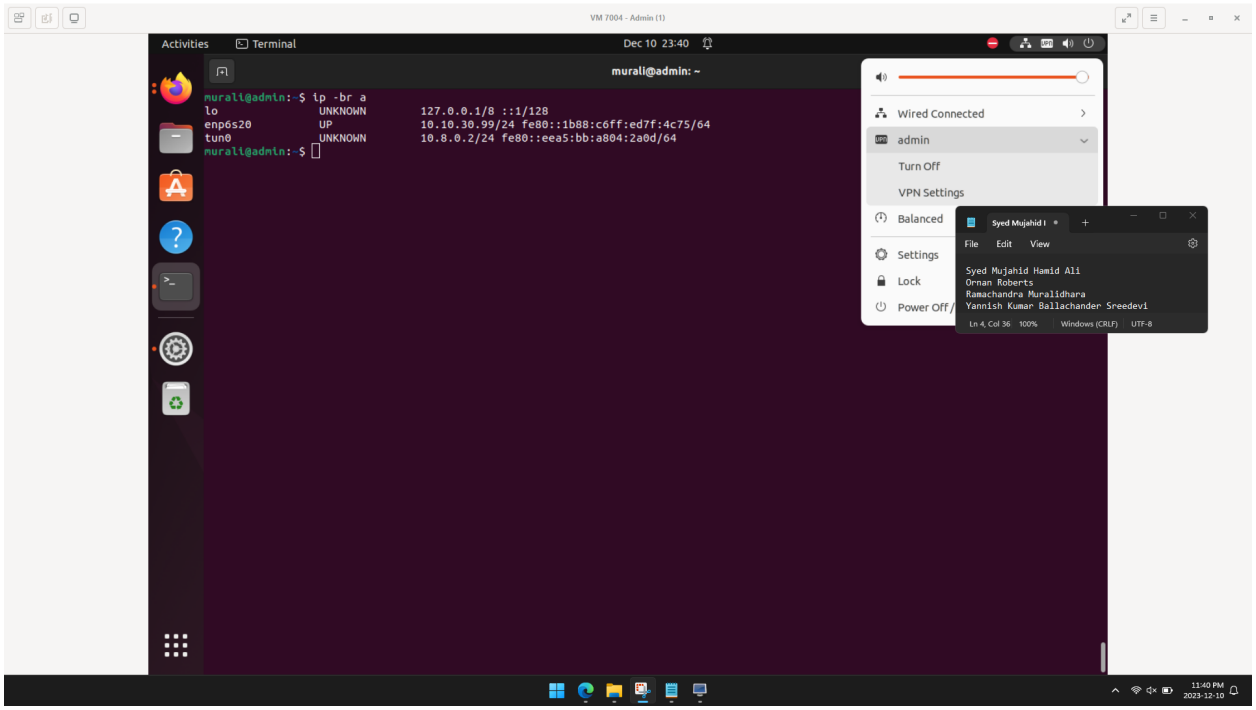
Selecting the Configuration File



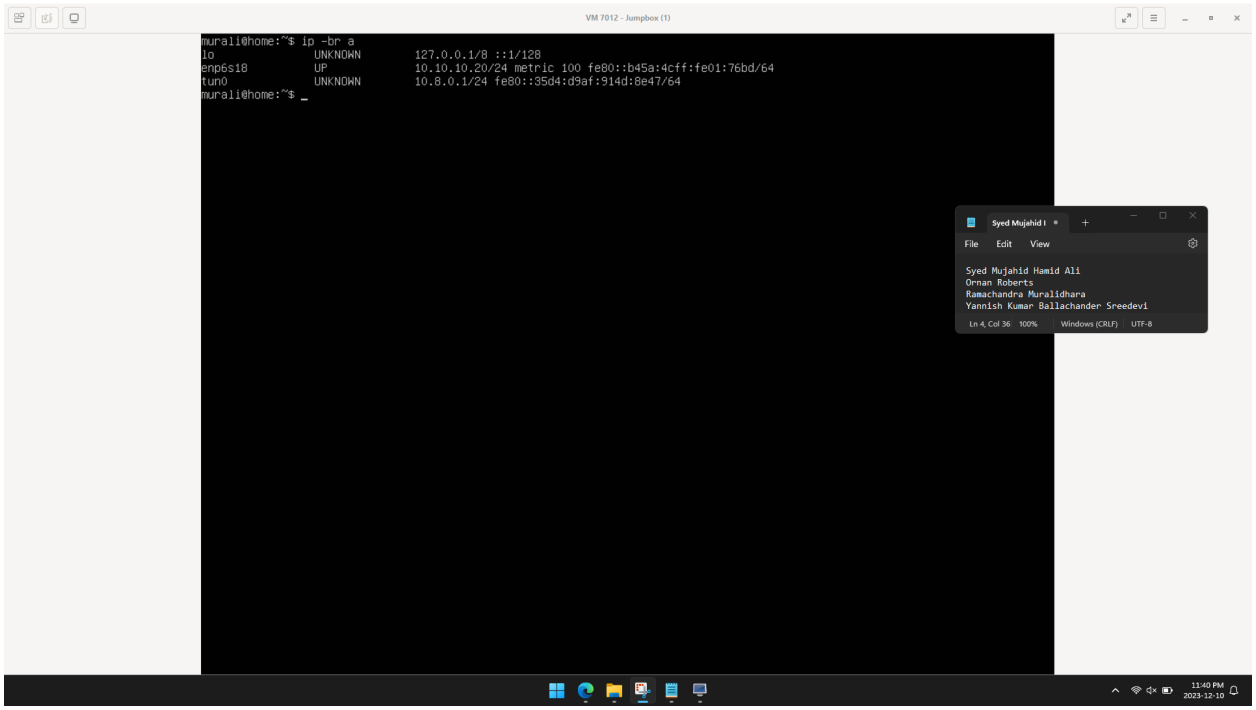
Adding the right certificates and other files



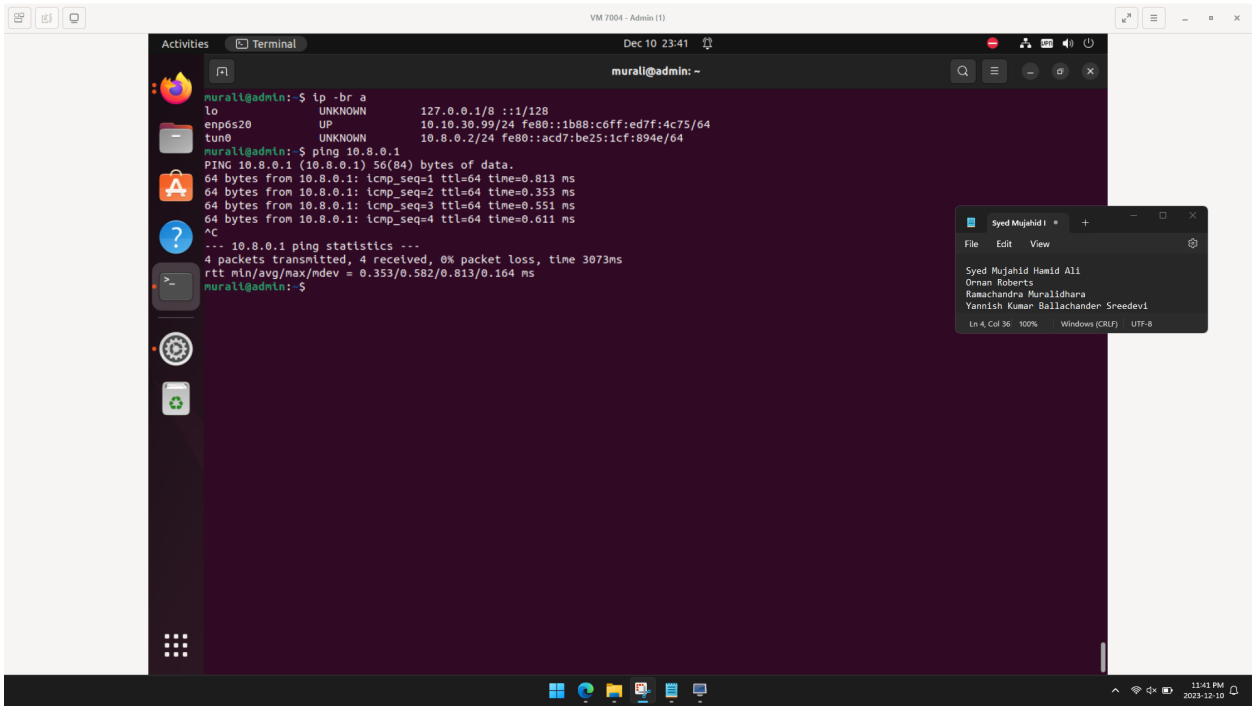
Tunnel interface created on Client when VPN is turned on



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.