LONDON METROPOLITAN UNIVERSITY

Islington college
(इस्लिङ्टन कलेज)

Module Code & Module Title

CS6P05NI - Final Year Project

Assessment Weightage & Type

40% Final Year Report

Semester

2022/23 Spring

Student Name: Janaki Chaudhary

London Met ID: 20049154

College ID: NP01NT4S210070

Internal Supervisor: Prasant Pudasaini

External Supervisor: Raman Pradhananga

Assignment Due Date: 19th April 2023

Assignment Submission Date: 19th April 2023

Word Count (Where Required): 10247

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submission and a mark of zero will be awarded.

Acknowledgement

First and foremost, I am very grateful to our Islington college for providing me with the opportunity and support to improve my skills and knowledge, which will be useful in, my future endeavors.

I would also like to express my deepest gratitude to my external supervisor Mr. Raman Pradhananga sir and internal supervisor Mr. Prashant Pudasaini sir, Mrs. Suman Gupta mam and Mr. Pratik Karki sir for their invaluable guidance, encouragement, and support throughout the duration of this project. Their expertise, feedback and suggestions have been crucial in shaping my ideas and ensuring the quality of my work.

Additionally, I would like to express my sincere appreciation to my parents and Everest Bank Lamahi (EBL) for their kind co-operation and encouragement which helped in the completion of this project. I am also thankful to my colleagues Bishwash Limbu, Pasang Dolma Tamang who have generously offered their assistance and expertise whenever I needed it.

Abstract

With the increasing prevalence of cloud-based environments and complex network of on-premised organization, the future holds immense potential for the network security solutions and automation. Automation will play a crucial role in asset management and software deployment in coming years. Automated asset management will enable organizations to track their hardware and software assets whereas automated software deployment will ensure all the systems running the latest software versions, reducing the risk of security vulnerabilities, eventually optimizing the performance. DMZ implementation is also a good security solution that can be deployed to protect against the network threats and data breaches. Overall, the future looks bright for network security solution and automation making the organizations to rethink their investments in right technologies and solutions.

The developed system will improve the security and efficiency of the network using a combination of network and software solutions, focusing on scalability and ease of maintenance. Moreover, this system will monitor the user satisfaction throughout the project to ensure the objectives are met. The system is expected to result in improved network security, increased efficiency and reduce workload for IT staff and administrator.

Regarding this report, it describes that this project is a client-based project in which the client was chosen, proposal was presented to him, and the project was replanned and created based on the client's requirements. This report is structured into different chapters, such as introduction that gives brief elaboration on the current topics, scenarios of both world and Nepal, a background chapter that explains how the system fulfills the client's needs and also the inclusion of prevailing similar projects and their comparison with this project, a development chapter that outlines the used methodology and its phases, the resources and design used in this project and implementation section that showing the configuration how the feature were implemented. Moreover, the testing phase includes multiple unit and system tests to ensure a functional and error-free system. Lastly, the conclusion the limitations, advantages and future work of the project and asserts that this project is ethically, socially, and legally sound for implementation.

Table of contents

Table of Figures

Table of tables

Table of abbreviations

IT	**Information Technology**
VM	**Virtual Machine**
DC	**Domain Controller**
AD	**Active Directory**
ADDS	**Active Directory Domain Controller**
HTTP	**Hyper Text Transfer Protocol**
HTTPs	**Hyper Text Transfer Protocol Secure**
DMZ	**Demilitarized Zone**
GUI	**Graphical User Interface**
RAM	**Random Access Memory**
EBL	**Everest Bank Limited**
LAN	**Local Area Network**
DG	**Default Gateway**
IP	**Internet Protocol**
DHCP	**Dynamic Host Configuration Protocol.**
DNS	**Domain Name System**
GNS3	**Graphical Network Simlator-3**
QEMU	**Quick Emulator**

CHAPTER 1: INTRODUCTION

The COVID-19 pandemic has led to an increased demand for virtualization and internet services, which has presented new challenges for network security. As more individuals and organizations rely on cloud-based applications and services, there is a greater risk of cybercriminals exploiting vulnerabilities in network security. Consequently, network security has become a crucial aspect of every organization, as it involves developing defensive strategies to protect data and resources from cyber threats. However, the current network architectures are complex and vulnerable to changing threats, leading to significant losses for organizations Therefore, a well-designed network security solution can reduce overhead costs and prevent costly data breaches and other incidents while ensuring legitimate access to systems, applications, and data (Barney, 2022).

There are different network security solutions among which the DMZ's are crucial component of network security. A DMZ (Demilitarized Zone) can be termed as a buffer zone between the internal and external network. Before the incoming traffic is allowed to enter the internal network, it is subjected to a thorough screening process conducted by security devices such as firewall and intrusion detection systems, which are deployed in DMZ. By implementing DMZ, organizations can reduce the exposure of their internal network to potential threats from external sources such as malware and hackers, thus ensuring the security and reliability of their network infrastructure (BasuMallick, 2022).

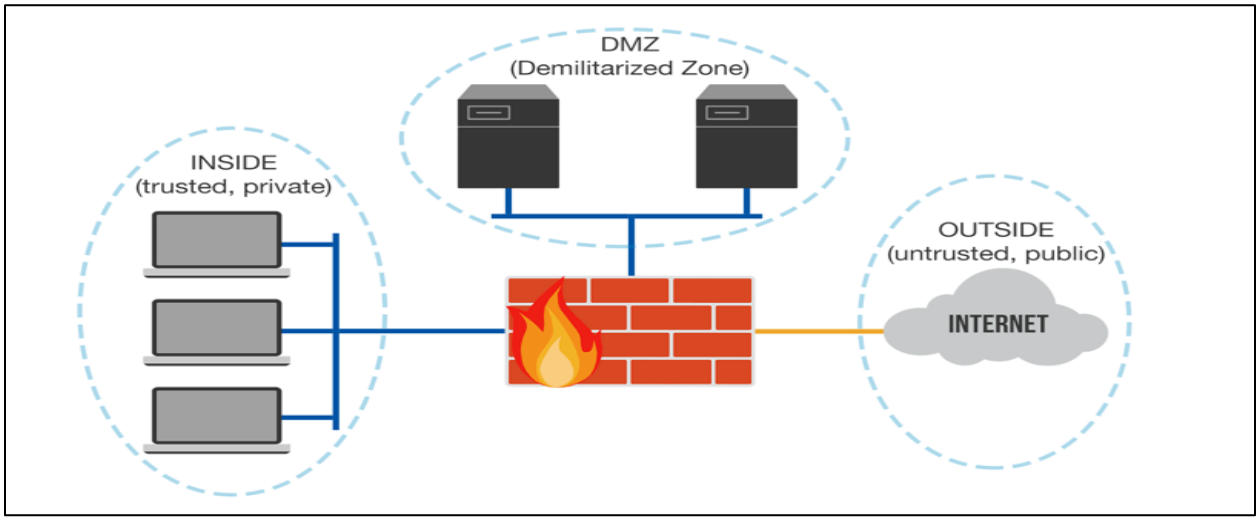


Figure 1 Demilitarized Zone (DMZ) (CyberHoot, 2020).

In present world, majority of organizations have complex network architectures, ultimately leading to chaotic and challenging asset management process. Asset management in a network refers to the process of tracking and managing hardware and software assets connected to the network. This may include identifying all devices and software installed on the network, tracking their location, managing licenses and warranties, and monitoring their performance and usage (Chouffani, 2023). There are different tools used for asset management process such as Lan Sweeper, Spiceworks, SolarWinds etc. Lan sweeper is a powerful asset management software that allows organizations to conveniently scan and manage all devices in the network. It can automate the scanning and tracking of hardware and software assets, as well as perform inventory management and license management (Kennedy, 2023).

Moreover, the complexity in network architectures not only raise asset management issues but also the time-consuming manual software installations and patch management. Patch management refers to the process of acquiring, testing, and installing patches on computer systems to prevent security vulnerabilities and maintain the performance as well as stability of the systems (Ayuya, 2023). Some popular tools used for software deployment and patch management are PDQ deploy, Ivanti Patch Management, SolarWinds patch management etc. PDQ deploy can be considered as the most user-friendly, convenient, and effective software deployment tool which enables automated software package installations and patch management to keep the system up-to date making it convenient and a very useful tool for system/network admins (Willlians, 2022).

1.1. Project description

The major topic of this project is development of a network architecture for the client of this project, Everest Bank Limited, located in Lamahi, Dang. The project aims to provide an integrated network solution that meets the specific needs of the organization. The integrated network solution provides a comprehensive approach to network security by creating a DMZ, enabling virtualization, implementing a domain controller for user authentication and access control, and deploying LAN sweeper and PDQ deploy for efficient network management.

Regarding the project elaboration, this project's entire work has been carried out on a single PC by utilizing virtualization tool i.e., the entire system is virtually developed and simulated. There is use of different network devices such as firewall, router of different vendors which will automatically uplift the security of the system. The firewall appliance is configured on gns3. Moreover, there is an additional server providing internet to the appliance i.e., gns3 VM server. A Debian 11 is configured as a web server by installing the Apache webpage. This web server is considered as the external web server which is used for further DMZ implementation. Overall, different firewall policies are deployed in order to create a DMZ zone for the security of internal network. The gns3 is used by thousands of people across the globe for emulation network projects.

Additionally, the router, Debian 11, Miktrotik router and VMware ESXi is implemented over VMware workstation 16. Within VMware ESXi, four VMs are configured i.e., domain controller, web server as internal web server and two windows clients. There is implementation of an asset managing tool Lansweeper and a software deployment tool pdq deploy. Moreover, the internal web server is also used for hosting internal website which is customizable for the internal users.

1.2. Current Scenario

1.2.1. World

The present world is entirely dependent on the internet and variant of high-tech. Almost every company's network is becoming complex and relying on numerous connected endpoints, thus allowing access for the malicious intruders inside company's network. As a result, the company faces monetary loss as well as the reputational damage of the organization is also downgraded in the marketplace. From the figure below, we can conclude that over these past years the malicious activities (network threats) have been increasing in rapid pace resulting in huge financial and reputational loss of different organizations globally. We can see the malicious activities has increased more than 20% over the past 7 years thus increasing the demand for network security (Zaharia, 2023).

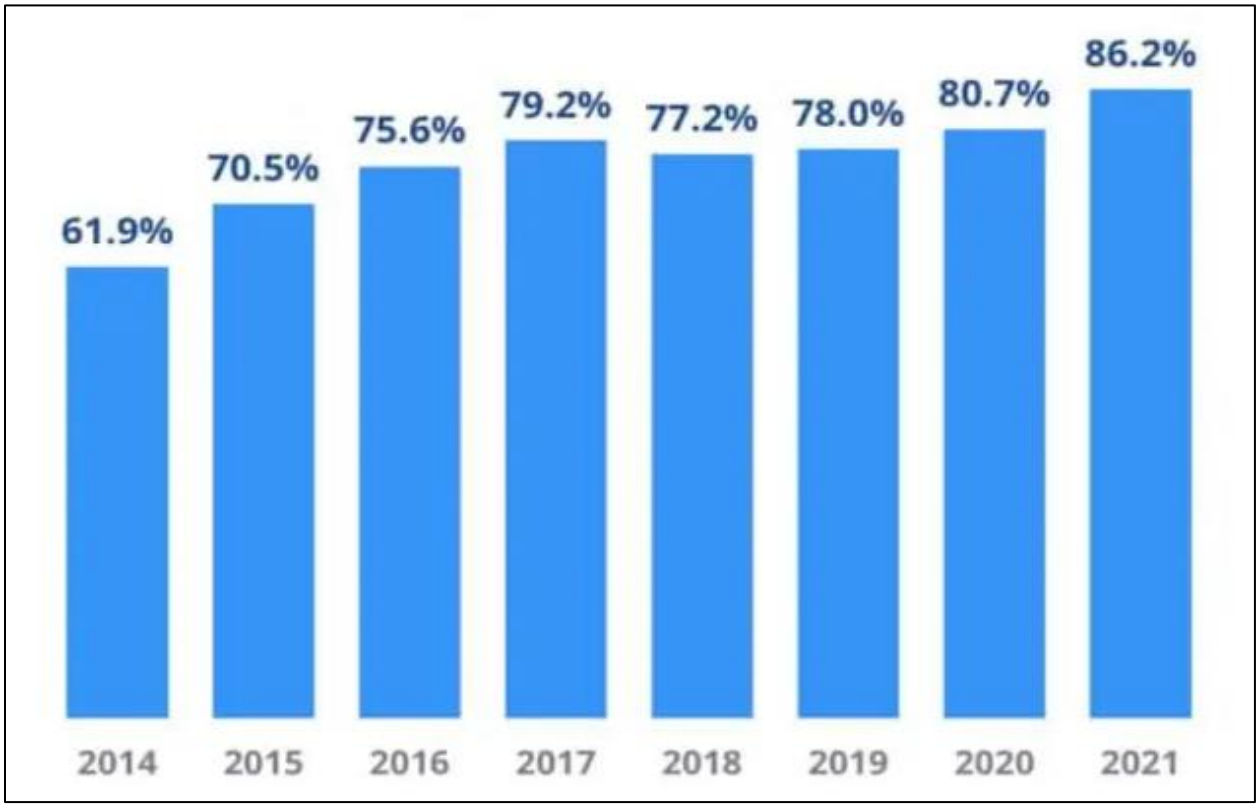


Figure 2 Percentage of organizations compromised in past years worldwide (Zaharia, 2023).

1.2.2. Nepal

Nepal is ranked 104th in digital entrepreneurship. Along with the advancement in technology, network/ cyber threats in Nepal are also increasing in rapid pace. While organizations in Nepal focus on competing for success and using the digitalization for marketing and promotion, overlooking the importance of IT security. This ignorance leaves the organization vulnerable to cyber criminals who seek to infiltrate and damage organizations (Prasain, 2022).

In developing country like Nepal, banks and online businesses are often the primary targets of cyber attackers and intruders. In 2017, the NIC BANK's IT server was hacked, resulting theft of millions of rupees. The banks never disable the remote terminal computers that were used for remote access and this vulnerability led to such a huge theft (Sharma, 2017).

Recently, there was a case where eight hackers were arrested for hacking into mobile banking app of NIC Asia (using mobile apps) and withdraw funds from various hacked accounts, ultimately stealing around 5 million from the bank (Nepal News, 2023). To avoid such occurrences, it is crucial for organizations to give priority to safety measures related to their IT and network infrastructures.

1.3. Problem domain and project as a solution

1.3.1. Problem domain

Since from past years, the network security issues have been increasing very rapidly. Many companies face different network security issues: DDOS attack, unauthorized intrusions, crucial data theft, ransomware etc. In most of the company the internal services and public services providing servers are kept in the same internal network. In this way the company is letting in people from an untrusted network (internet) and are given access behind the company's firewall. Hackers can use this as opening to cause havoc on the company's network. Since, the internal network devices are just behind the firewall, the hackers can try an access other sensitive data behind the firewall or even they can try a virus implant which is a security concern.

Additionally, in network environment asset management pose a significant challenge. The absence of assent management system/tools can result in difficulties in maintaining an accurate inventory of devices and software on the network, which can lead to a range of issues including security vulnerabilities, difficulties in troubleshooting networks problems, and challenges in maintaining compliance with industry regulations. Moreover, manual inventory tracking can be time consuming and prone to errors, leading to inaccurate or incomplete asset inventory which even make it more difficult to monitor and maintain the network's health and security (Kennedy, 2023).

Similarly, managing and deploying application packages and software updates manually in a network environment can be challenging task. It can be time-consuming to perform manual software/ application deployments and even the process can be prone to errors resulting to security vulnerabilities.

Moreover, with the increasing use of cloud services and wireless devices, traditional asset management tool. Practices and software deployments are no longer sufficient. Majority of the organizations are now, have to manage assets and perform package installations located outside their physical premises, making them more complex.

To conclude, both on-premises and cloud-based organizations encounter challenges with system/network security, asset management and software deployments.

1.3.2. Project as a solution

This project will assist in resolving the problem stated above. Since, there is implementation of DMZ for external service providing server i.e., web server which will isolate the web server from the internal network. This can help to prevent unauthorized access to sensitive information and resources in internal network. The network administrators can easily control the access to server by opening the necessary ports and protocols only. Additionally, placing the web server will also simplify the management and monitoring of network traffic by providing a clear separation between internal and external network traffic which can help to identify and isolate any suspicious activity or potential security threats.

Similarly, the installation of domain controller will ease the centralized management of user accounts, groups, and policies. It will also make more secure environment for user authentication and authorization as well.

For eradicating the asset management problem, Lan sweeper will be implemented inside the internal LAN. The Lansweeper is an asset scanning and managing tool that simplifies the asset management process by providing a comprehensive detail of all the devices and software present in the network. It will also save the time as well as the results are less prone to errors thus forming a healthy and secured network environment (Kennedy, 2023).

Similarly, to overcome the difficulties of manual application or package deployment, we will be using PDQ deploy on web server. By suing it, we can easily deploy the application or packages simultaneously in different AD user's computer at once. It acts as a centralized deployment.

Overall, the implementation of this system and tools can greatly enhance the security and productivity of both on-premises and cloud-based organizations, enabling better management of the complexities of contemporary network infrastructure.

1.4. Aim and Objectives

1.4.1. Aim

The main aim of this project is to develop and demonstrate a virtualized system that safeguards the security of internal network, centrally manages the network elements like user and policies, streamlines asset scanning and management and enables automated software deployment and patch management, ultimately enhancing the organization's network features, it can be for those organizations that are dealing with network threats, manual and lengthy asset management and software deployments and other system administration related problems.

1.4.2. Objectives

The objectives of the project are,

- To reduce overheads of cost, maintenance, power consumption and space by using virtualization.
- To reduce the potential network threats by deploying a DMZ zone that isolates external service providing server from the internal network and restricts access to sensitive resources.
- To facilitate centralized control over users and policies by implementing a domain controller.
- To organize the internal network elements like users, computers, and other devices into a hierarchical container structure for better organization and management.
- To streamline the process of asset scanning and management present in the network via Lansweeper tool.
- To enable automated software package deployments via PDQ deploy.
- To minimize errors and security risks that are caused by manual deployments.
- To automate patch management for keeping the devices up to date using PDQ deploy.

1.5. Structure of the report

1.5.1. Chapter 1: Introduction

In the introduction section, there is brief explanation about this project. There is brief elaboration about the current situation also, Moreover, the problem domain is elaborated along with the proper solution measures applied in this project to tackle the problem. Lastly, this part includes the major briefing i.e., the aim behind implementation and development of this project and the objectives that are going to be fulfilled in this project.

1.5.2. Chapter 2: Background

The background section of the report provides a brief description about the client and clients requirement's to be implemented in this project. It also explains a better way of understanding the project all the features and overall description of the project. Additionally, it presents brief elaboration about similar projects along with the comparison table and a in depth analysis, this part also elaborates the technical aspects of the projects.

1.5.3. Chapter 3: Development

Development includes discussion of several methodologies considered and selected methodology along with the justification for choosing and not choosing the methodology. Additionally, phases of the selected methodology are described. Moreover, the designs: physical logical diagrams, flowchart, use case diagrams are also included in this section.

1.5.4. Chapter 4: Testing and analysis

This section includes the test plans, test cases according to the test plans and screenshots for justifying the test cases. Additionally, a critical analysis of the test plans and cases is also elaborated.

1.5.5. Chapter 5: Conclusion

This chapter includes the overview of the project's report along with the legal, ethical, and social issues that may be caused due to implementation of this project. Furthermore, it also includes a description of a future works/ improvements for this project.

CHAPTER 2: BACKGROUND

2.1. About the end-user

2.1.1. Client description

- **Clients Name**: Prabin Subedi

- **Description of the client**

  The client of this project is Mr. Prabin Subedi. He is currently working as a Branch Office manager at Everest Bank Limited in Lamahi Dang, Nepal. Everest Bank Limited is a commercial bank in Nepal and has its headquarters in Kathmandu. The EBL has been providing customer friendly services through its wide Network connected through ABBS system from 1994 thus helping the nation to develop corporately, agriculturally, and industrially, contributing to the economic development of Nepal.

  Mr. Prabin has consented to serve as the project's client since he believes this project would be beneficial and feasible for enhancing office's network features.

Figure 3 Everest Bank Limited's logo (client's logo) (Everest Bank Limited, 2023).

The client's approval letter has been presented in section 8.8. Appendix G.

2.1.2. Client Requirements

- **Use of virtualized network simulation**

  As per the client, he has asked to present a virtual demo of the suggested network architecture. The virtual representation of the system will help in clear understanding and adding or removing the features as per the requirement.

- **DMZ implementation for internal network security.**

  The client has requested to implement DMZ and isolate their external service providing network elements in DMZ zone to enhance their internal network security.

- **There should be use of network devices from different vendors.**

  There should be inclusion of network devices from different vendors to enhance the organization's network feature as well as security also.

- **Use of virtualization**

  There should be use of virtualization tools and techniques to reduce the cost and resource management overheads.

- **There should be use of Domain controller.**

  There should be centralized control over the users/client using ADDS service to simplify the management of the network components.

- **Convenient asset management.**

  There should be deployment of asset scanning and managing tool to help the IT officers and admin to manage the infrastructure by providing factual information about the devices connected to the network.

- **Automatic software package deployment and patch management.**

  There should be use of software deployment tool to automate deployment of the packages/ application among AD users simultaneously. The system should be able to automate the patch management to ease and save the time of administrators.

2.2. Understanding the solution

2.2.1. System overview

This project provides a virtual demonstration of network architecture using network simulation tool and type-2 hypervisors. The network architecture includes a DMZ implementation on an external web server using FortiGate firewall which limits the external user (internet user) access to web services only, thus preventing the internal network potentially from malicious attackers. Additionally, a domain controller is configured within the LAN for centralized control of users and policies. Moreover, an internal web server is configured which can host private website among the internal users. To sum up, a LAN sweeper tool is implemented on internal web server that scans and manages assets/ network infrastructure present in the network. Finally, a PDQ deploy tool is also implemented to ease the software, applications, or packages deployment in multiple AD users simultaneously saving the time.

2.2.2. Solution for End users

Firstly, the main goal of this project is to present a network architecture that enhances the security as well as eases the network features of the client company. To achieve the project goal, a reliable system (network architecture) is developed that resolves the issues listed during the research phase and through direct engagement with client. The system provides security to the internal network as well as enhances the network features with easy asset management/ scanning and simultaneous, scheduled, and automatic package deploy. The figures (5 and 6) which are given below clarify the system overview clearly,

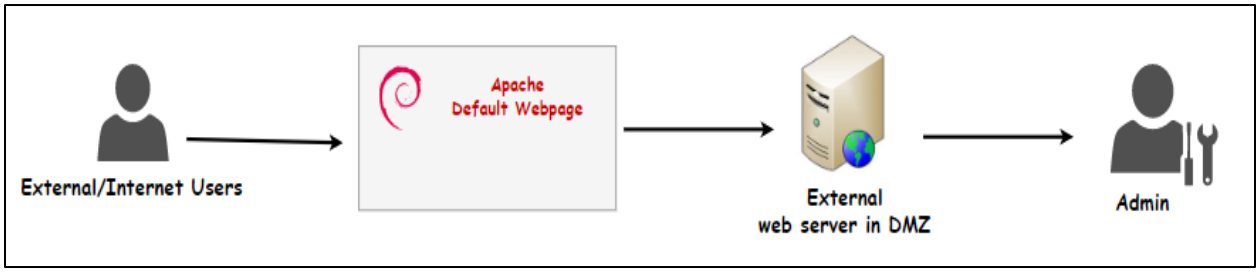


Figure 4 System overview1 (DMZ zone)

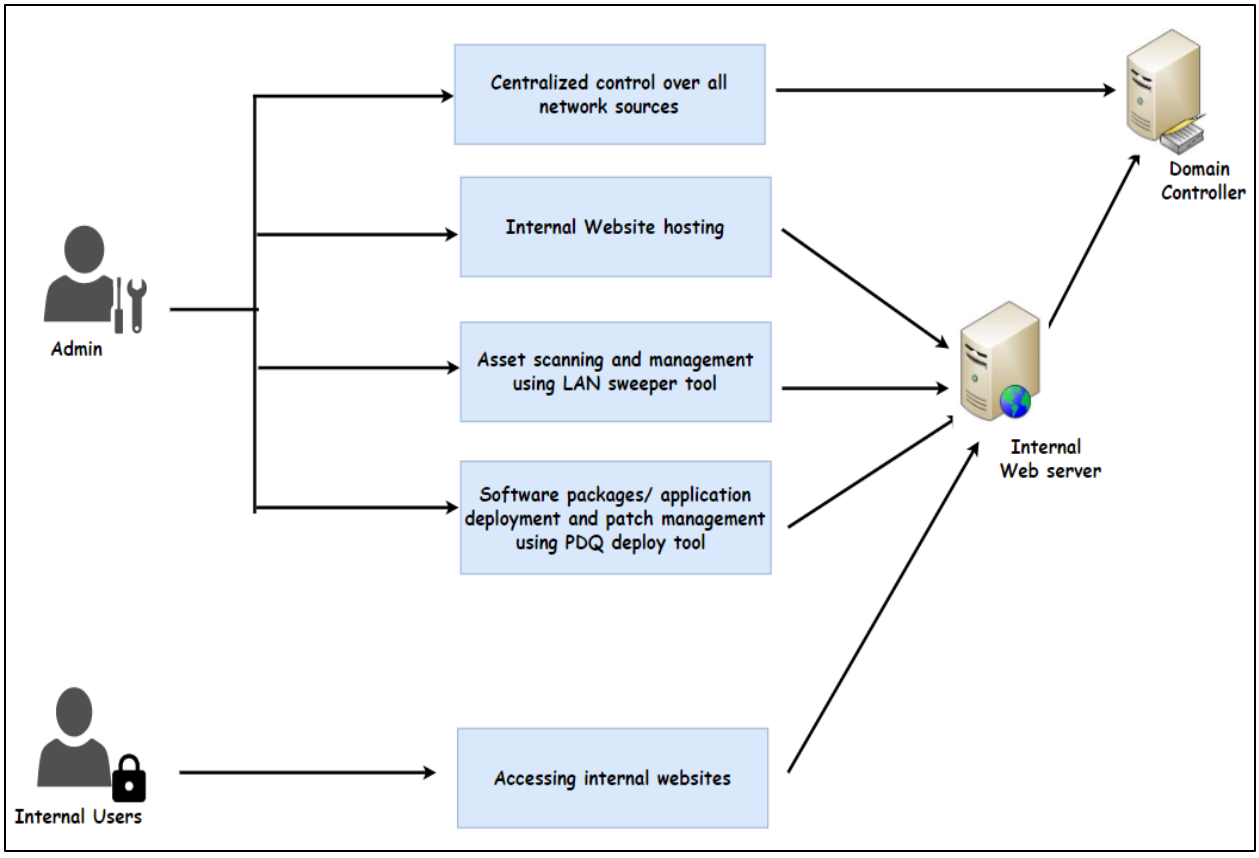


Figure 5 System overview2 (Internal network)

2.2.2. Features and functions.

2.2.2.1. Virtualization

This project employs virtualization technology for demonstration. For the virtual demonstration, a virtual network simulation tool gns3 and type-2 hypervisors i.e., VMware workstation and VMware ESXi 7 are used. Though the gns3 is just used for the testing and demonstration purpose but use of these hypervisors offers many benefits for organization of all sizes. It facilitates the reduction of hardware maintenance and costs by running multiple virtual machines on a single server, allowing for easy backup, and enabling easy scaling of resources to meet changing demand without the need for additional hardware. Additionally, it also simplifies the management of IT resources by allowing admin to conveniently manage virtual machines and allocate resources.

2.2.2.2. Demilitarized zone

Generally, DMZ is used to host publicly accessible servers. In this project's scenario the external web server is placed in the DMZ of the FortiGate firewall. The external web server can be used to host websites such as company blogs, for banking instance, it can be online banking and other services providing websites, for the External/internet users. Thus, the web server is separated from internal network as shown in the figure below and the firewall is configured to allow only HTTP and HTTPS traffic to pass through the internet and blocks all other traffic. Moreover, the firewall is also configured to allow the web server to communicate with the necessary internal network services, blocking access to other resources in internal network.

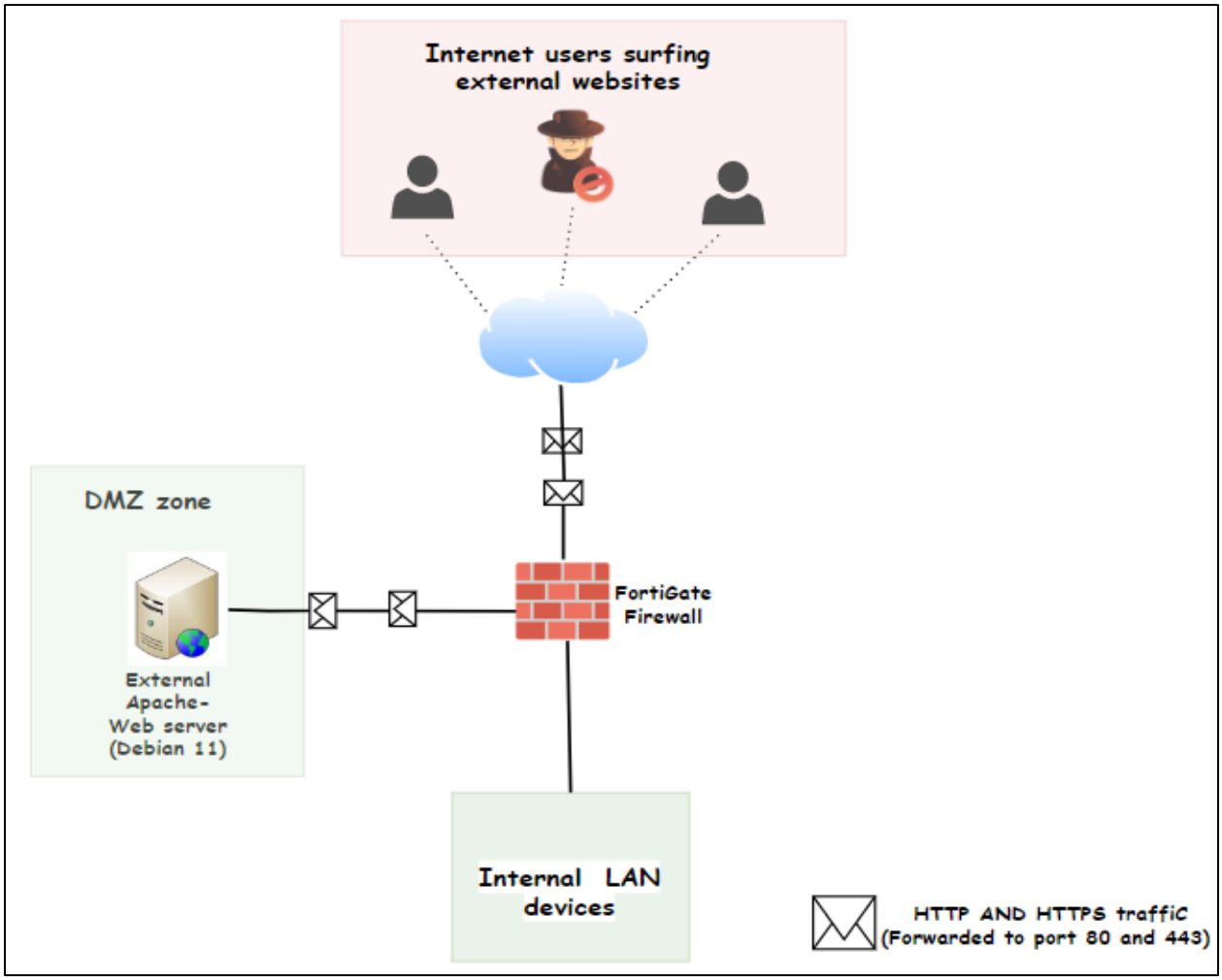


Figure 6 DMZ working Scenario of the system.

2.2.2.3. Domain controller

In this project, the domain controller is configured as VM (Virtual Machine) in VMware ESXi 7. A new forest EBL.com is created and under this domain, an internal web server and two windows computers as a user are configured subsequently. The domain controller provides central management of user accounts. Security policies and access control, reducing the risk of security breaches. It also simplifies the user authentication and authorization. Overall, this domain controller will enhance the network features by streamlining management, improving security, and providing centralized control.

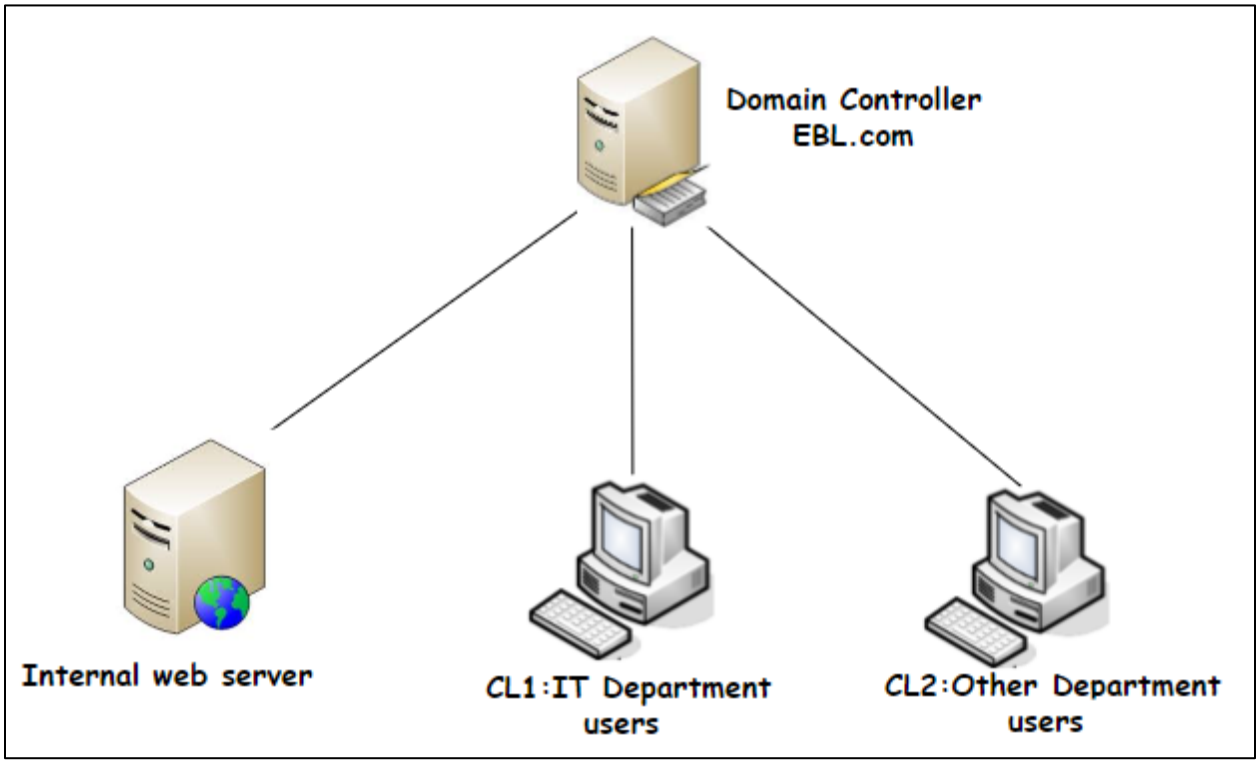


Figure 7 Domain controller and devices added to EBL.com domain.

2.2.2.4. Internal web server

The web server is under the EBL.com domain. On internal web server, a website is hosted for internal users which can be furthermore customized as per client requirement. Moreover, the server is set up with two tools- LAN sweeper and PDQ Deploy, which are versatile and beneficial for both on-premises and cloud-based network. Lansweeper simplifies the asset management while PDQ deploy enables manual, automated and schedules package deployments, resulting in time savings and streamlined workflow. The internal website can also be customized as per the needs and requirements of the client.

Figure 8 Internal web server

2.2.2.5. Asset management via Lansweeper.

The Lansweeper needs to be installed on the web server. After the successful installation, it scans the network and gather information about the different hardware and software present in the LAN. Additionally, it also provides alert about the issues of any devices in the network. The GUI is user-friendly thus the administrator of the organization can conveniently utilize this tool. Overall, this tool is affordable compared to other options in the market, making it smart choice for organizations of any size.

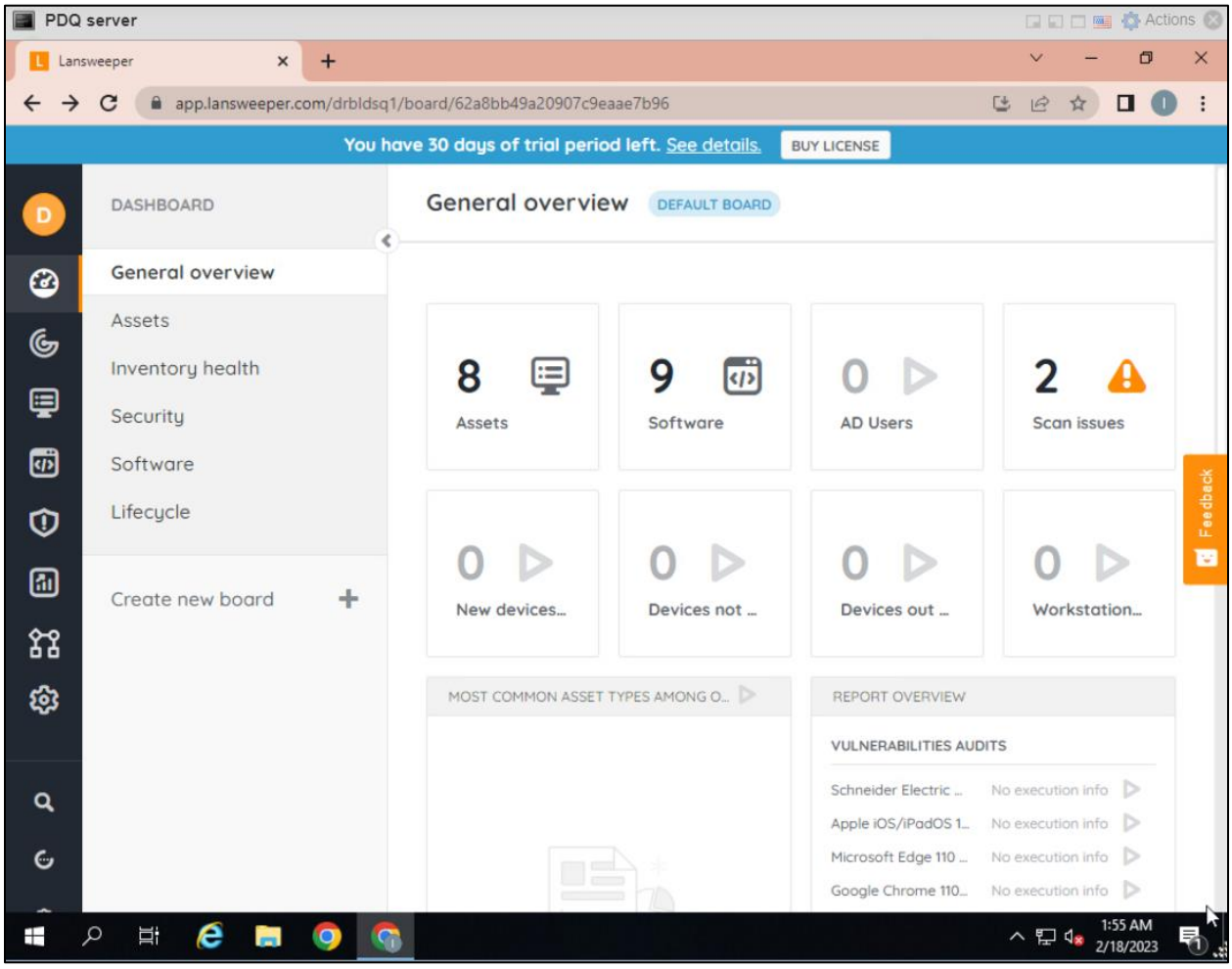


Figure 9 User-friendly interface of LAN sweeper

2.2.2.3. Software deployment automation and patch management with PDQ deploy.

The PDQ deploy tool eases the work of the network/ system administrators by automating patch management. This tool allows manual as well as scheduled software/ packages deployments. Manual deployment requires admin to initiate the deployment process while scheduled deployment can be set up to run automatically at specific times/events. Moreover, the admins can also choose specific Active directory users or groups to receive packages. It also offers real time updates and error reporting to help administrators to track the progress of the deployment. Using this tool can save time and reduce errors by automating the software deployment process (clearfind, 2023).

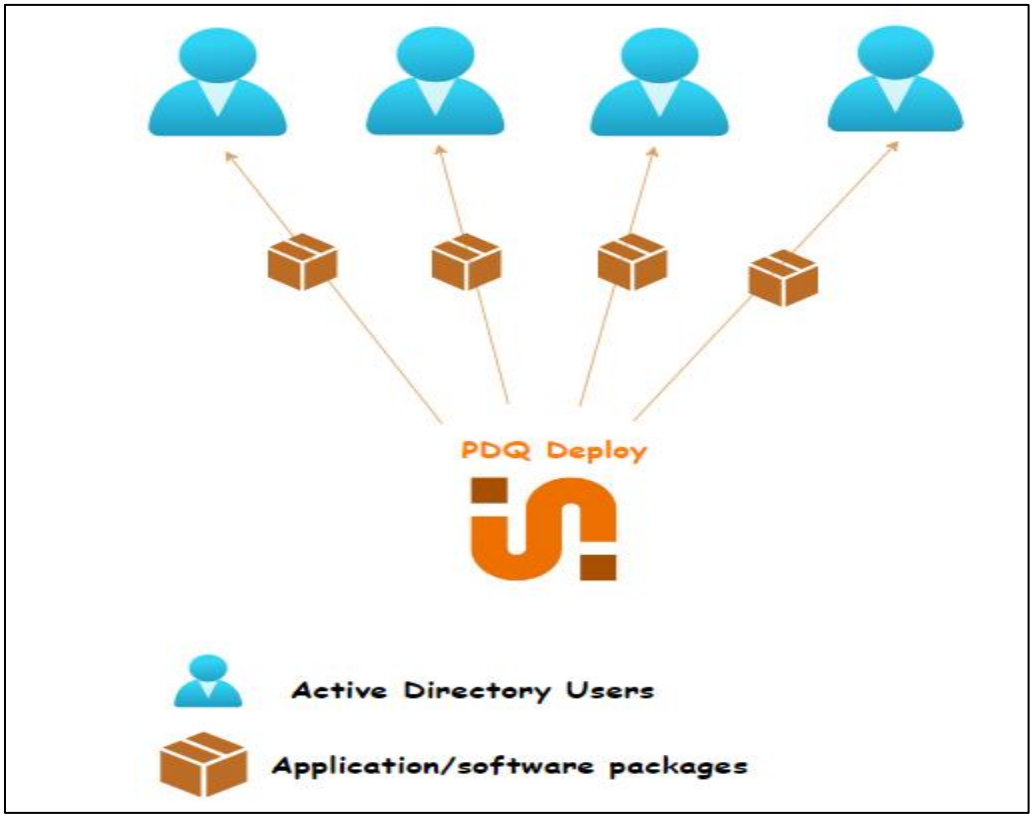


Figure 10 Package deploy scenario using PDQ deploy.

2.4. Similar projects

2.4.1. Project 1: Demilitarized Zone: Network Architecture for information Security

This project was implemented to provide security to the confidential information of the servers and internal network. In this project a separate network (DMZ) was created which provided security without affecting the accessibility of the data, this project was simulated in gns3 using dual cisco router, public server, dual VPCs and internal server. In this project, the internal server and pcs were kept in DMZ so that if any attacker gets success in obtaining an access inside trusted network, cannot access the DMZ network as shown in the figure below (Shrimali, 2017). In the figure below, we can see that if the hacker is able to access in the public server, he/ she will not be able to get access into the internal system behind the internal router. Thus, protecting the servers and internal Pcs from unauthorized access.

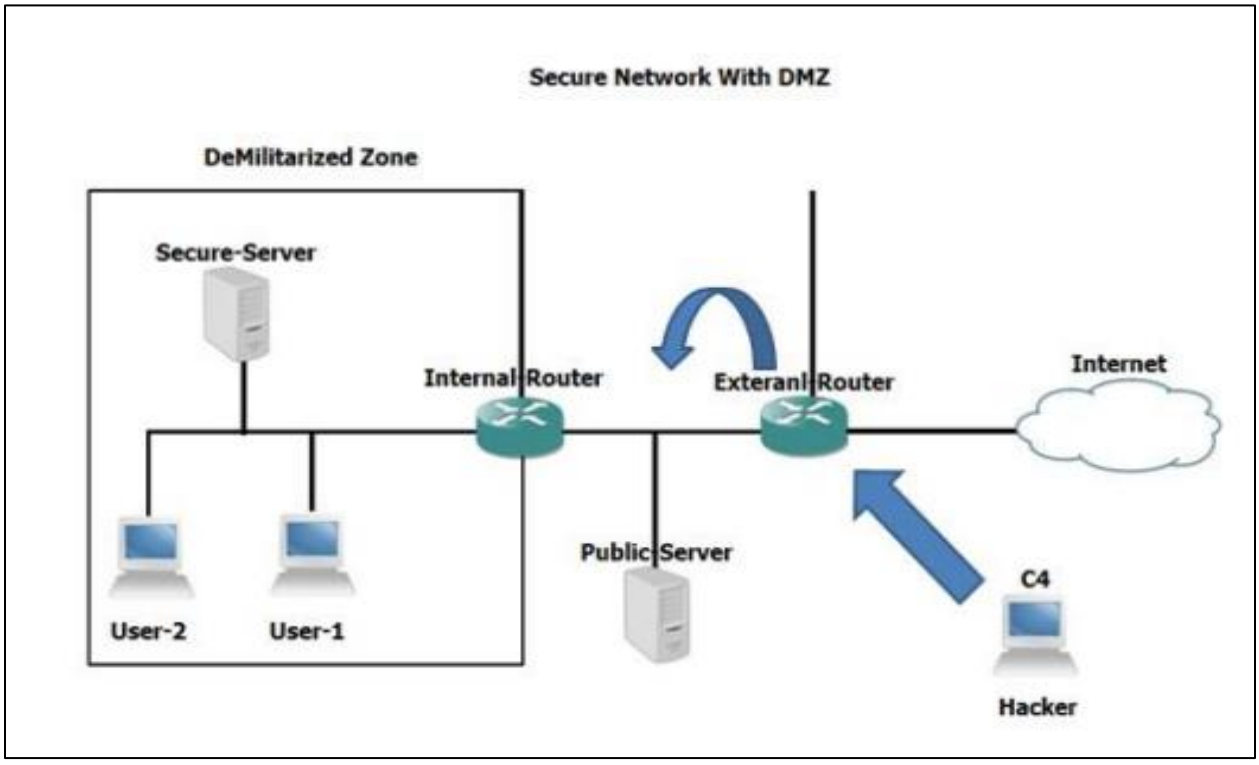


Figure 11 Similar project 1 (Shrimali, 2017)

2.4.2. Project 2: Firewall implementation and Testing

The main objective of this project is to set up a virtual environment for the implementation and testing of firewall like DMZ and other penetration testing. To simulate this project, there is use of 10 virtual machines each running its own functionalities. Among the ten VMs, three server VMs were kept in DMZ, five VMs were kept in LAN, one VM acted as an external host and one firewall was connected to all the subnets as shown in figure below. Regarding the DMZ testing, we can see that the external service providing servers i.e. mail server, web server and DNS server are kept in DMZ and external host will get all the external services from the servers kept in DMZ thus protecting the internal LAN servers and internal system from the unauthorized access to the internal LAN (Pratik Ragnarson, 2018).

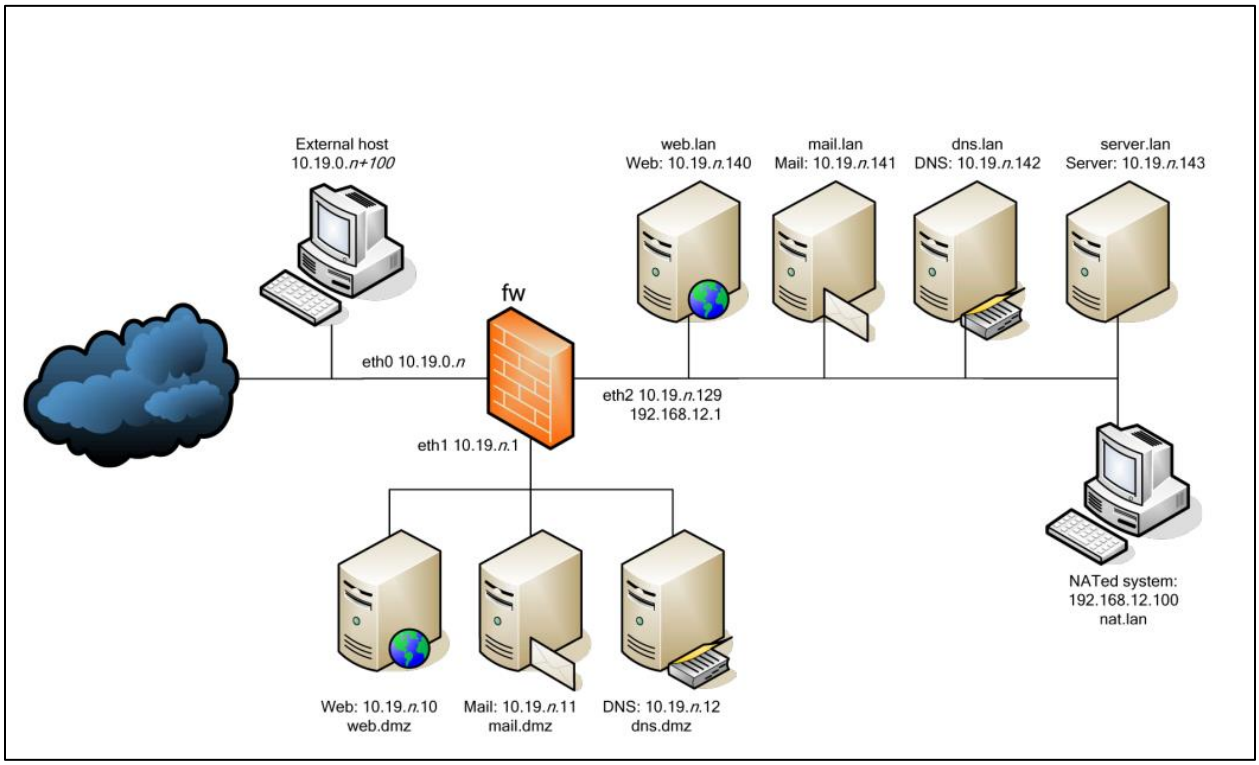


Figure 12 Similar project 2 (Pratik Ragnarson, 2018).

2.4.3. Project 3: Demilitarized Zone: An exceptional Layer of Network Security

In this project, two different networks are created to demonstrate two different scenarios i.e., the external network with no DMZ implementation and internal network with DMZ implementation. Overall, the project is divided into three sub networks i.e., internal network that consists of the confidential severs containing sensitive and web server that provides web services to the external network. Meanwhile the external network consists of the external users and employee machines. There is sue of cisco Asav firewall for configuring the DMZ zone as shown in the figure below. Generally, the external services providing servers are kept in DMZ zone but in this project's scenario, the internal network treats DMZ network as an outsider i.e., if the web server inside DMZ zone wants an access to internal network, then it must have permissions to bypass the firewall to enter internal network thus preventing the internal network from malicious attacks (Patel, 2020).

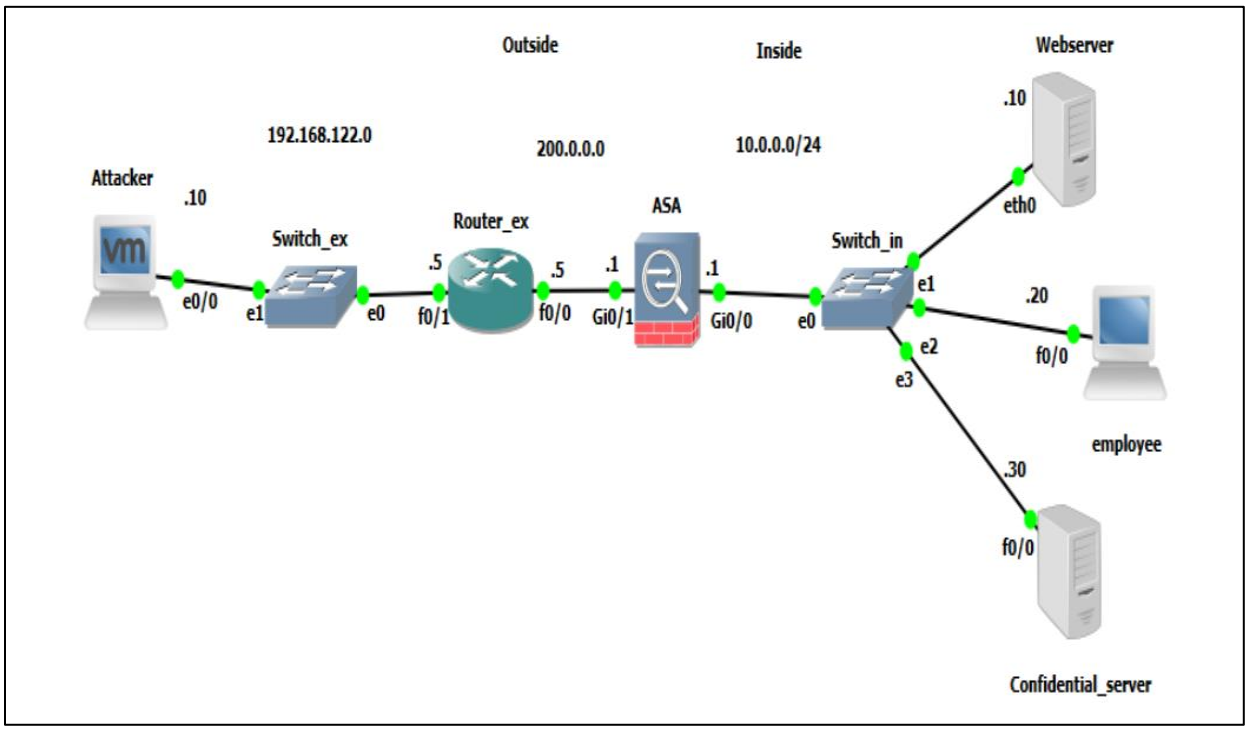


Figure 13 Similar Project 3 (Patel, 2020).

2.4.4. Comparison between the similar projects

S.N.	Features	Project 1	Project 2	Project 3	This project
1	Simulation tool	Gns3	Virtual box	Gns3	Gns3
2	Easy to install	✓	**X**	✓	✓
3	Use of virtual hypervisor VMware ESXi.	**X**	**X**	**X**	✓
4	Use of network devices from different vendors.	✓	✓	**X**	✓
5	External host/ attacker	✓	✓	✓	**X**
6	Use of firewall for DMZ configuration.	**X**	✓	✓	✓
7	Use of LAN sweeper	**X**	**X**	**X**	✓
8	Use of domain controller	**X**	**X**	**X**	✓
9	Use of PDQ deploy	**X**	**X**	**X**	✓

Table 1 Comparison table of similar projects.

2.4.5. Critical evaluation of the comparison table

Analyzing all the features from the similar projects as show in the table 1. This project can be considered as the refined project in virtualization of the similar projects. There is use of gns3 as network simulation tool in project 1 and 3 as like this project. The project 2 is using only virtual box which makes it very difficult to maintain the virtual network adapters as well. Moreover, this project includes an asset scanning tool LAN sweeper, domain controller for managing users and departments of the client company as well as PDQ deploy tool for the package deployment in the AD (Active Directory) users enhancing the network structure and features of the client company.

CHAPTER 3: DEVELOPMENT

3.1. Considered methodologies.

3.1.1. Waterfall methodology

The waterfall methodology is a linear project management approach that is widely used and was the first process model developed. It is known for its simplicity and ease of use, making it popular choice for software development. This methodology follows a sequential workflow where each phase of the process must be completed before proceeding to the next and the phases also must not overlap as well. In this methodology the requirements are well understood before initiating the project as the changes to the requirements can be difficult and costly (Leeron Hoory, 2022). The separate phases of this methodology are shown in figure below,

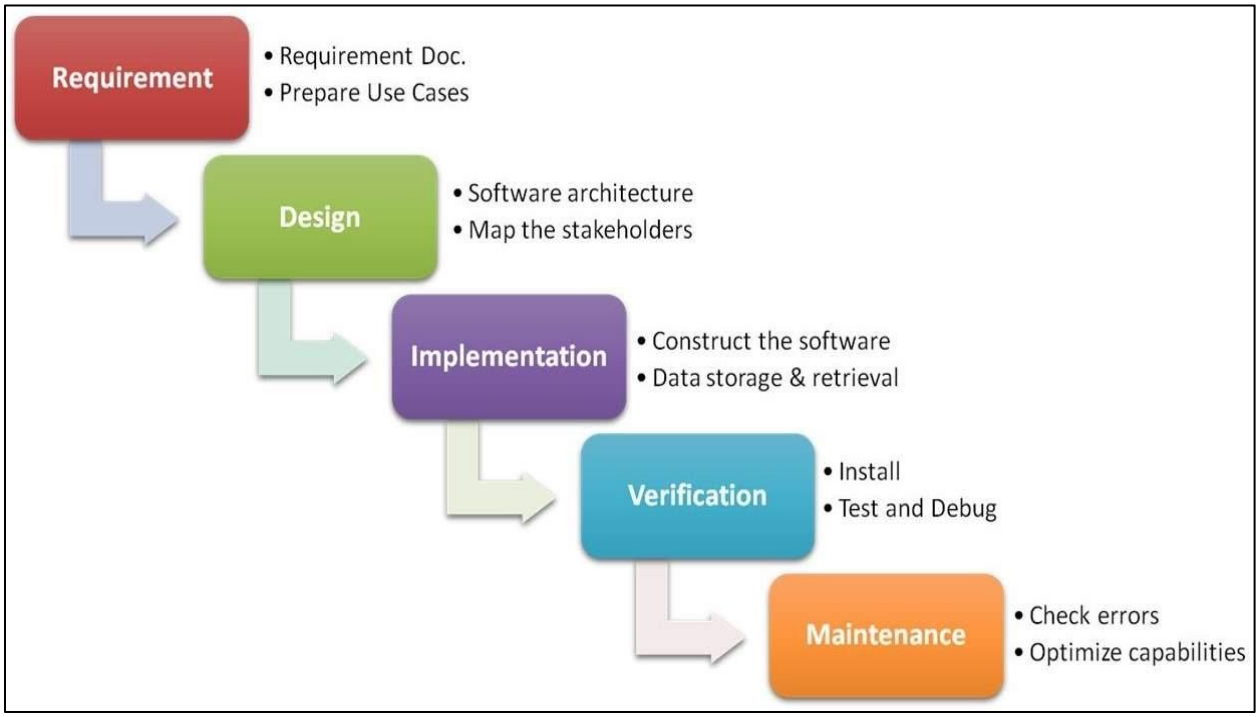


Figure 14 Waterfall methodology (UKessays, 2019).

Advantages of the waterfall methodology,

- Being one of the oldest models in software development, waterfall methodology ensures that a comprehensive product is delivered if executed correctly.
- This methodology is a good fit for small projects with defined requirements, fixed budgets, and timelines, as it offers a clear route to completion.
- The waterfall approach is straightforward and easy to comprehend, making it suitable for developers of all levels.

Disadvantage of waterfall methodology are,

- The inflexibility of this methodology can lead to inefficiencies and delays, as it does not permit changes or modifications to be made after the completion of a phase.
- The linear and sequential approach of this methodology of this methodology poses a risk of delivering an outdated or inadequate product, especially in rapidly evolving industries.
- This methodology suits smaller projects.

The reasons for not choosing this methodology are:

- Since, this is a client-based project, there will be changes in the requirements, but this methodology follows a linear approach which may create difficulties to make changes and adapt the new features.
- Since, this project spans a year, use if this methodology can lead to an outdated deliverable.
- It cannot deliver a functioning product until the end of the project's lifecycle.
- It does not support the idea of revisions as a result the development cycle is restarted if a flaw is found during any stage.
- The inability to adapt changes according to client post feedback may result in client dissatisfaction.

3.1.2. Agile methodology

Agile methodology is an iterative and incremental approach to software development that prioritizes customer satisfaction, teamwork, and flexibility. It involves short development cycles called sprints and emphasizes responding to change, regular communication, and continuous improvement. Unlike waterfall methodology, it is suitable for smaller projects for quick implementation. For large projects, it is difficult to estimate the development time as it requires a strong coordination with developers as well as joint analysis of planning and requirement. The agile approach is widely used in the software industry to increase efficiency, adaptability, and customer satisfaction (Hamilton, 2023).

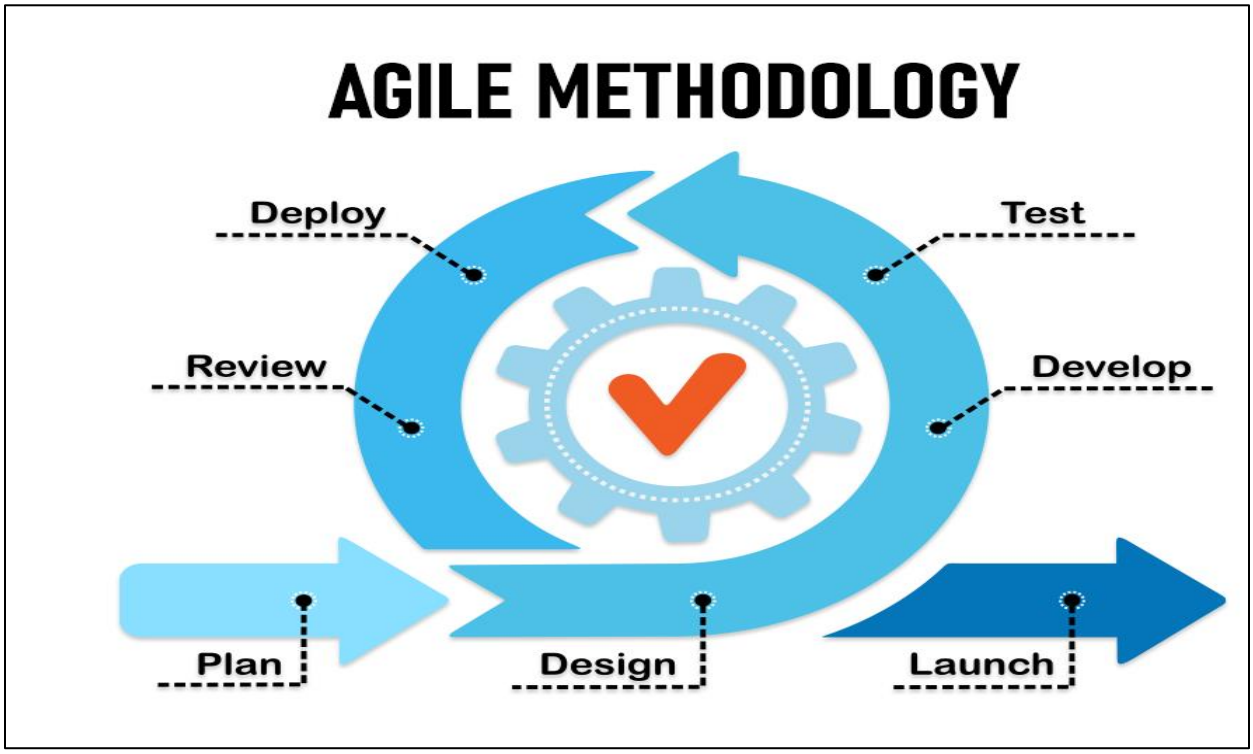


Figure 15 Agile methodology (Mohanan, 2022).

Advantages of agile methodology,

- This methodology prioritizes customer satisfaction by involving then in the development process and by providing then with working product at the end of each sprint.

- It offers flexibility and collaboration by adapting changing requirements and emphasizing teamwork among cross-functional teams.
- The efficiency of the project is increased by breaking the development process in short sprints.

Disadvantages of the agile methodology are,

- The flexibility and adaptability to changes can cause difficulties to estimate the completion time and overall cost of project.
- This methodology requires experienced people to work on to make decisions and prioritize tasks.
- Since this methodology focus on customer satisfaction, can lead to scope creep when the customer frequently requests changes.

Reasons for not choosing this methodology are,

- This project is a solo research project, and it does not involve the participation of multiple members, but this methodology requires involvement of multiple experienced team members.
- The initial designs and development of this are finalized making it difficult to breakdown the project into sprints.
- The initial requirements are also not gathered with accordance to the client's feedback making it difficult to make further decisions.
- The limited availability of user feedback in this project due to a busy schedule makes it impossible to hold multiple meetups in every sprint.
- The project has a deadline to meet, so it requires a fast development process and breaking it down into sprints would consume a lot of time.

3.1.3. Evolutionary prototyping

Evolutionary prototyping is a software development strategy that focuses on adaptability and ongoing enhancements. It involves building an initial simple design and prototype of the system and then refining it through client feedback and their requirement i.e., to make the project more efficient, practical, and marketable, new features can be added and old features can be deleted. This iterative process allows for changes to be made easily during the development process, making it a valuable approach for complex or innovative projects. Evolutionary prototyping encourages collaboration and innovation leading to the development of high-quality system/prototype that meets user needs (Martinez, 2023).

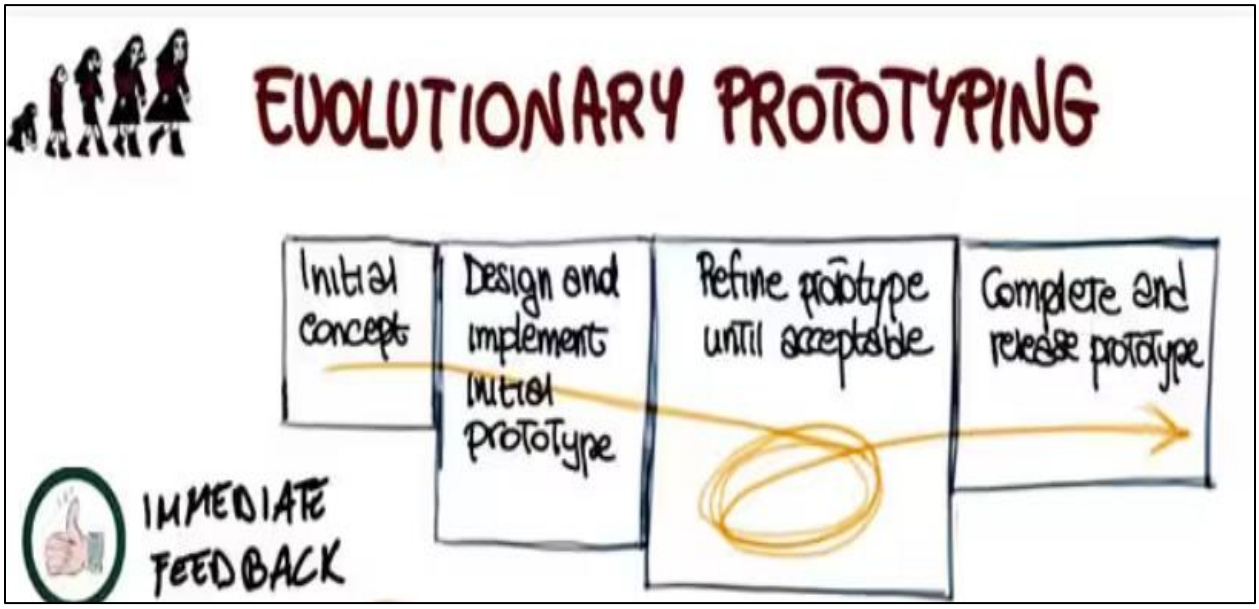


Figure 16 Evolutionary Prototyping (Agelica, 2023).

Advantages of evolutionary prototyping

- The design of this methodology is adaptable.
- Error is easy to spot.
- Functionality lacking can be quickly located.
- There is room for improvement i.e., the new requirement can be accommodated quickly.
- It doesn't need a team/ group of professionals to work in.
- It can be utilized by the developer in the future for more complex system.

- This methodology helps to reduce software development costs by addressing issues early, which is more cost-effective than later fixes.

Some disadvantages of evolutionary prototyping are,

- The final system's complexity may increase.
- This model is a slow process.
- Huge documentation and reports.

Reasons for selecting evolutionary prototype,

- Since, the proposal was prepared without any client's requirement, so this methodology was a good fit for further changes and adaptations.
- Early feedback in evolutionary prototyping helps identify and address issues early in the development process.
- The continuous feedback and improvement process can lead to a better product that satisfy the needs and expectation of client.
- The system can be utilized in future for developing more complex system.

The brief elaboration for selecting evolutionary prototyping methodology is presented below, in selected methodology section.

3.2. Selected methodology

3.2.1. Evolutionary prototyping

The evolutionary prototyping approach was chosen for this client-based project due to the need for flexibility to incorporate changes and new ideas. The proposed design was created with current market situation in mind but will require refinement and modification. The iterative and adaptable nature of evolutionary prototyping is ideal for this project because it allows continuous improvement, which can be better meet the client's need over time. Additionally, the prototype can be altered multiple times to accommodate unclear or evolving client requirements. This approach also encourages feedback and criticism from internal and external oversight.

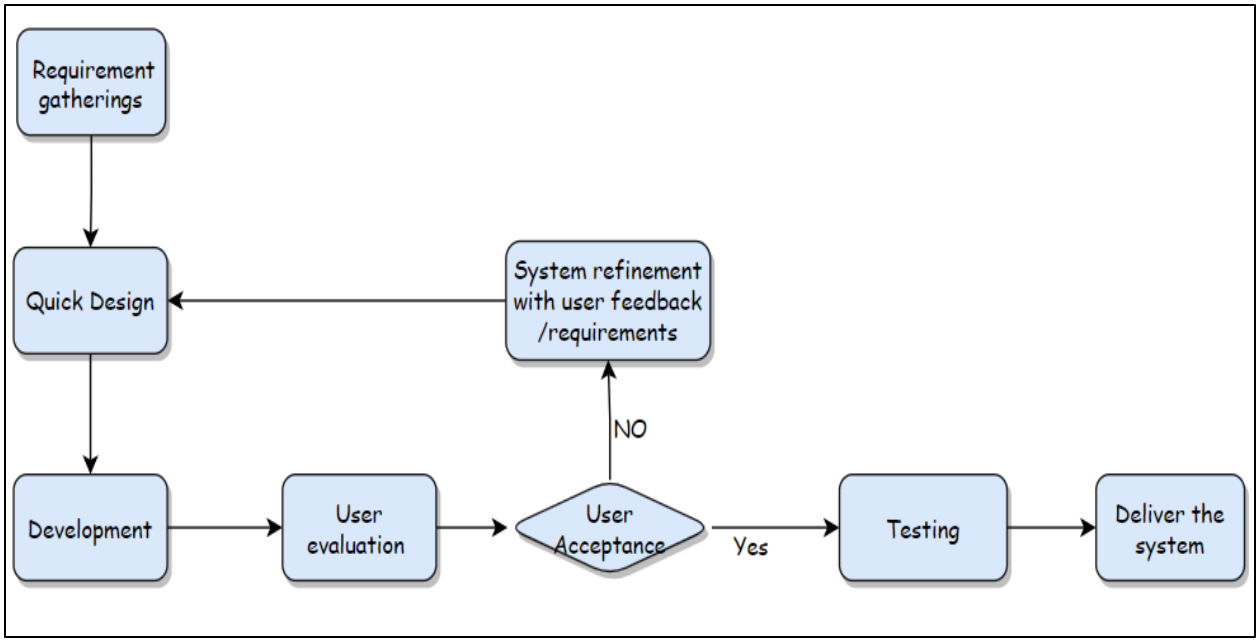


Figure 17 Evolutionary prototyping phases with regards to my project.

As shown in the figure above, the initial requirement gathering, and research will be carried out and a proposed design will be presented to the client. Then with the approval, the initial development will be done and again presented to the client for further feedback. Then a refined system will be developed by gathering the client's feedback and requirements. The refined system will be presented to the client and if the system is adequate then it will be implemented as final system and tested as well, and the final system will be delivered which satisfies the client's demands.

3.3. Phases of methodology

3.3.1. Requirements gatherings.

The initial stage of the methodology begins with thorough research into the project that aligns with the prevailing market demands. Furthermore, similar projects are researched and evaluated if such projects exist and suitable for the market. Subsequently, the required resources for the project are identified and estimated. A client is selected, and a meeting is scheduled. Then, a draft proposal design is presented to the client. Finally, the feedback and requirements of the client are noted down for further process. The steps involved in this stage are clearly depicted in the figure below, providing a more explicit understanding of the process.

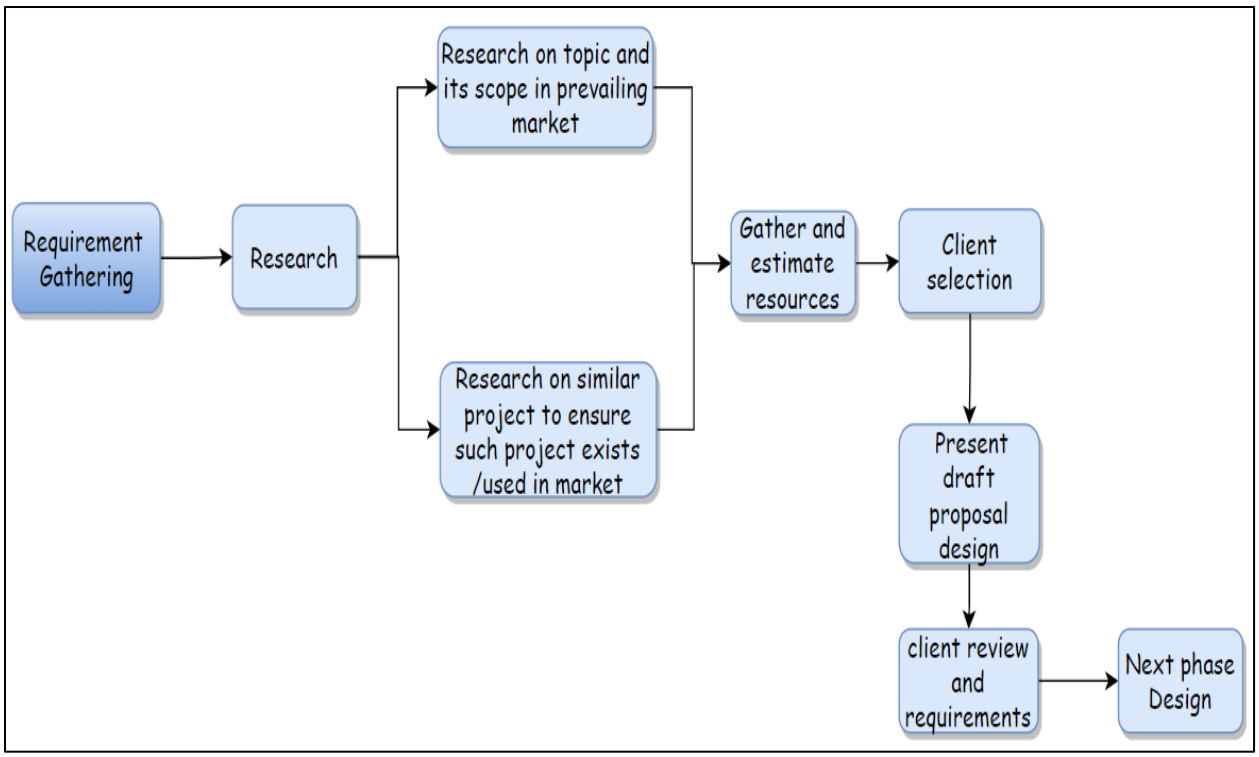


Figure 18 Requirement Gathering

The initial requirements gathered from the client is presented in the section 2.1.2.

The proposal draft design is presented in section 8.5.3. Appendix E

3.3.2. Quick Design

This phase includes the designing of the network architecture of the system. The network architecture was designed in accordance with client's requirements which were previously listed. The architecture was designed using tool draw.io. Additionally, a Gantt chart was also designed using a tool Gantt project to ensure that the project should be completed within the specified timeline. This phase was repeated once to improve the system's architecture as well as due to software incompatibility, utilizing the same resources/tool used before.

The initial design used for the development is presented in section 8.5.4. Appendix E.

The final system design used for development of final system development is presented in section 3.6.1.

3.3.3. Development

This phase includes the development of the design approved by the client and the supervisors. Initially, the first design was developed partially and presented to the client for further feedback. After the feedback, a final development work was done with addition of new requirements made by the client.

The screenshot of the development of initial system is presented in 7.3: Appendix C

The screenshot of the development of final system is presented in 7.4. Appendix D.

3.3.4. User feedback and requirements

This phase includes the meetings with the client and their feedback or any new requirements/suggestion to be implemented on the system. The meeting was arranged two times after the development. Despite of busy schedule, Mr. Prabin Subedi and his IT officer Milan Regmi were available for the meeting. Firstly, the draft design as proposal was mailed. After getting the approval letter, feedback and their requirements, the new design was created and developed.

In the pre-online meeting, the system that had been developed was showcased to the client. They requested the inclusion of a software deployment tool which could deploy software/packages to

all internal users at the same time, to eliminate the issue of manual installation. This additional requirement was noted down and the refinement process was initiated. In the post online meeting, again the developed system was presented for the feedback. This developed system was accepted by the client.

The letter of approval for initiation of system development is presented in Appendix G.

The Q/A for initial requirement gathering's is presented in section 8.6.1. Appendix E

The Q/A and feedback and requirement of the pre-online meeting is presented in section 8.6.2. Appendix E

The Q/A and feedback and requirement of the post-online meeting is presented in section 8.6.3. Appendix E

3.3.5. Refining system

After the pre-online meeting, the additional requirement was listed. Furthermore, refinements in designing of the network architecture was dome. Following the finalized design, the development was also done. Finally, an improved system was developed which fulfilled all the pre and post requirements of the end user(client).

.

3.3.6. Testing

The testing phase is critical phase of this methodology. In this phase, the final system is implemented and thoroughly tested to ensure that it is error-free and functioning correctly. Different types of testing such as unit testing and system testing are performed to validate the system's functionality. Unit testing involves individual testing of the different components used in the system and system; s testing involves the functionality of the features implemented in the system. Overall, this phase ensures that the system is reliable, stable and performs as expected before it is delivered.

The unit and system testing of the final system that are done is presented in the section CHAPTER 4: TESTING.

3.3.7. Deliver the system.

This phase includes the delivery of the final system/product to the client.

In the end, after rounds of refinements and testing, a system which can enhance the security and network features of the client company was delivered. The delivered system met all the requirements and features mentioned by the client.

The final system overview is presented in section 2.2.2.

3.4. Survey results

For the purpose of system development and improvement, surveys are crucial in gathering feedback from users. These surveys help in analyzing requirements and obtaining feedback on the product. In this context, a presurvey was conducted with a sample size of 21 participants, and a post survey with a sample size of 73 participants. This feedback helped me to identify areas for improvement and better understand user needs. The feedback from the participants has been documented in the following sections.

3.4.1. Pre-survey results.

- Majority of participants have faced network threats issues in their organization.
- 60% of people were known about DMZ.
- Majority of the people believed that virtualization will be the best solution to reduce overheads of cost maintenance power consumption and space.
- Majority of people were convinced that this project will minimize the chances of network threats.

Results of pre survey has been provided in the section 7.1: Appendix A

3.4.2. Post-survey results

- Majority of people have noticed improvements in the system's security after the DMZ and ADDS implementation.
- Many participants agreed the use of LAN sweeper eases the asset management.
- Nearly all participants, found the PDQ deploy convenient and user friendly.
- Majority of the people have given positive response about the performance of overall system.

Results of post survey form has been provided in the section 7.2: Appendix B

3.5. Requirement Analysis

3.5.1. Hardware requirement

The system is developed in a virtual environment with no specific use of hardware. For the implementation of this project, my personal laptop (Dell G3 3500) with following hardware specifications is used,

- 16 GB RAM
- Intel(R) Core (TM) i7-10750H CPU @ 2.60GHz 2.59 GHz
- 64-bit operating system, x64-based processor

3.5.2. Software requirement

The software requirements for this project are,

3.5.2.1. For planning and development tracking

- Gantt Project

3.5.2.2. For system development

- GNS3 and GNS3 VM
- VMware Workstation 16
- VMware ESXi 7
- Firewall
- Router
- Switch
- Windows server 2019 and 2022
- Debian 11 Linux
- Lan sweeper
- PDQ deploy.
- Windows 7 enterprise

3.5.5.3. For documentation and presentation

- Microsoft office.

The in-detailed description of the software used in this project is presented in section 8.7. Appendix F.

3.5.3. Functional requirements

The functional requirements for this project are,

- Maximize the computer utilization.
- Minimize the overheads of cost management, power consumption, maintenance, and physical space.
- Isolate external-facing components from the internal network.
- Restrict access to sensitive resources of the internal network and allow access only to required services.
- Centralized control and management of user accounts and policies.
- Scan and manage assets connected in the network environment.
- Generate reports and alerts or any credential issues related to the assets.
- Deploy software packages and updates across multiple computers in a centralized way.
- Scheduled package deployment and automate patch management.

3.5.4. Nonfunctional requirements.

The non-functional requirements for this project are,

- Error free system
- System security
- Compatible with the client's network infrastructure.
- User-friendly
- Customizable

3.6. Design

3.6.1. System architecture (Physical topology)

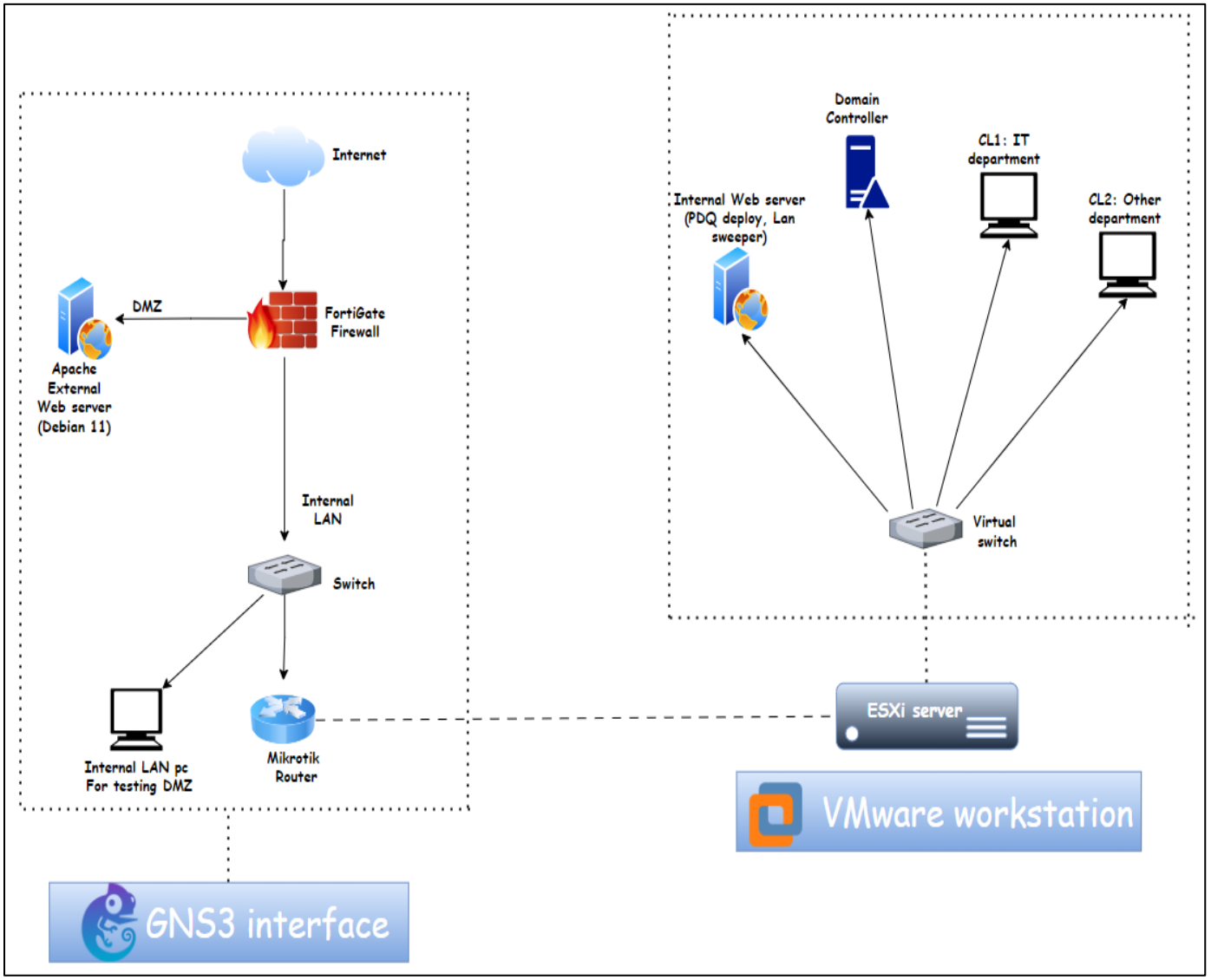


Figure 19 System architecture (physical topology)

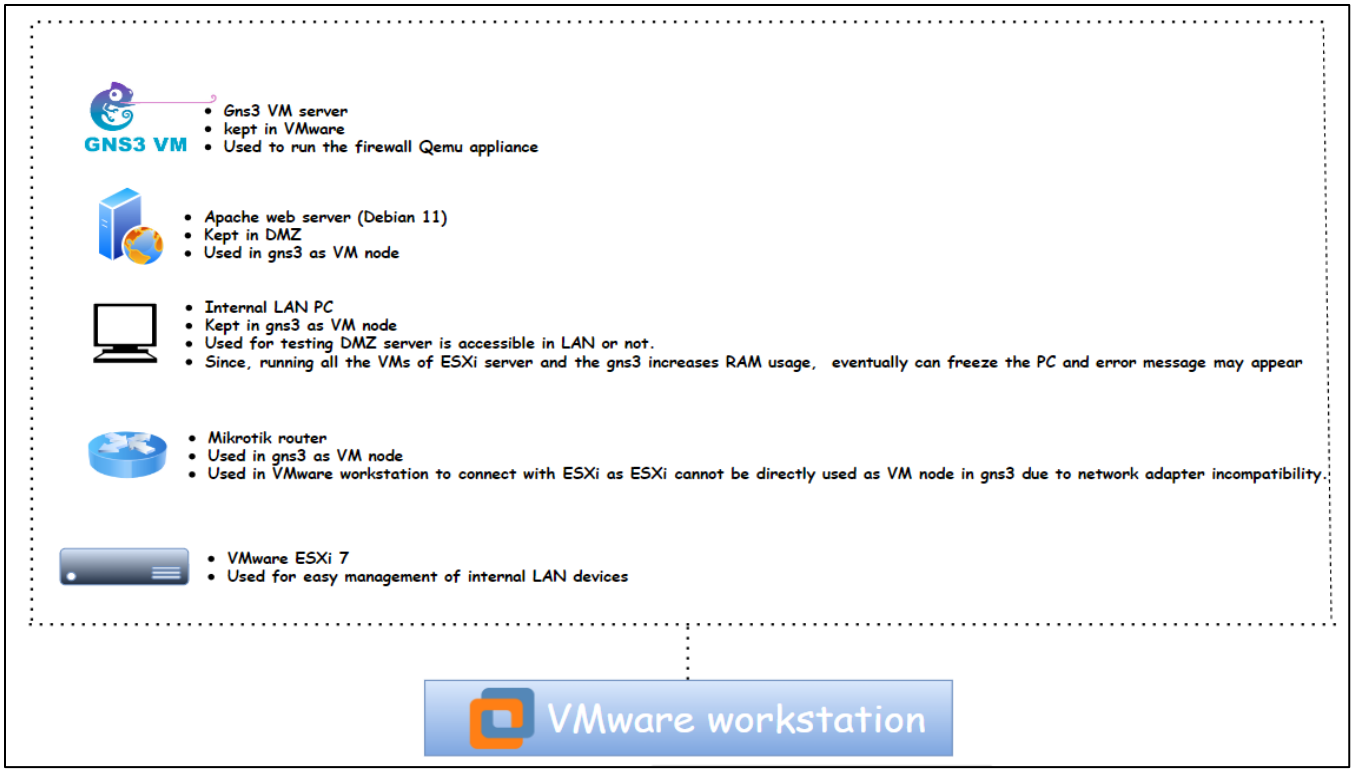


Figure 20 Inside VMware workstation

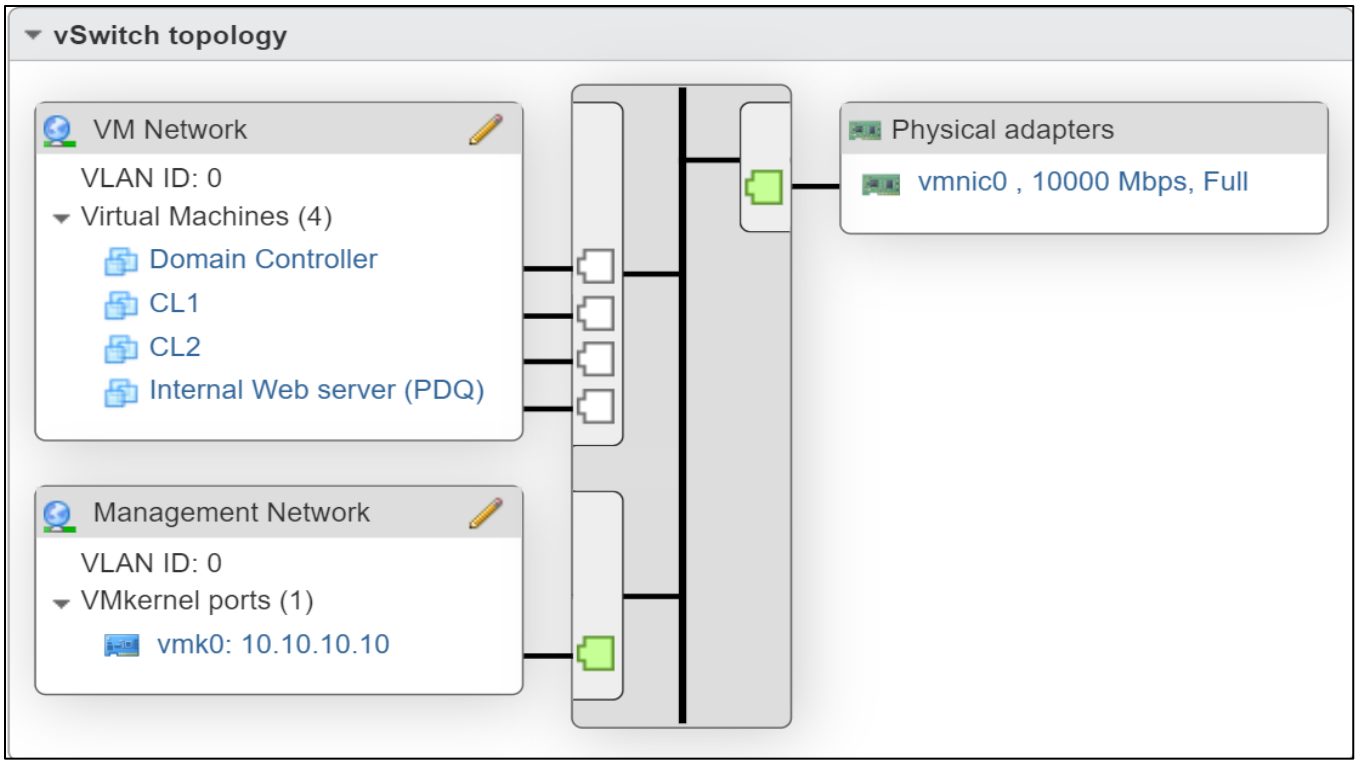


Figure 21 Inside VMware ESXi 7.

3.6.2. System architecture (logical topology)

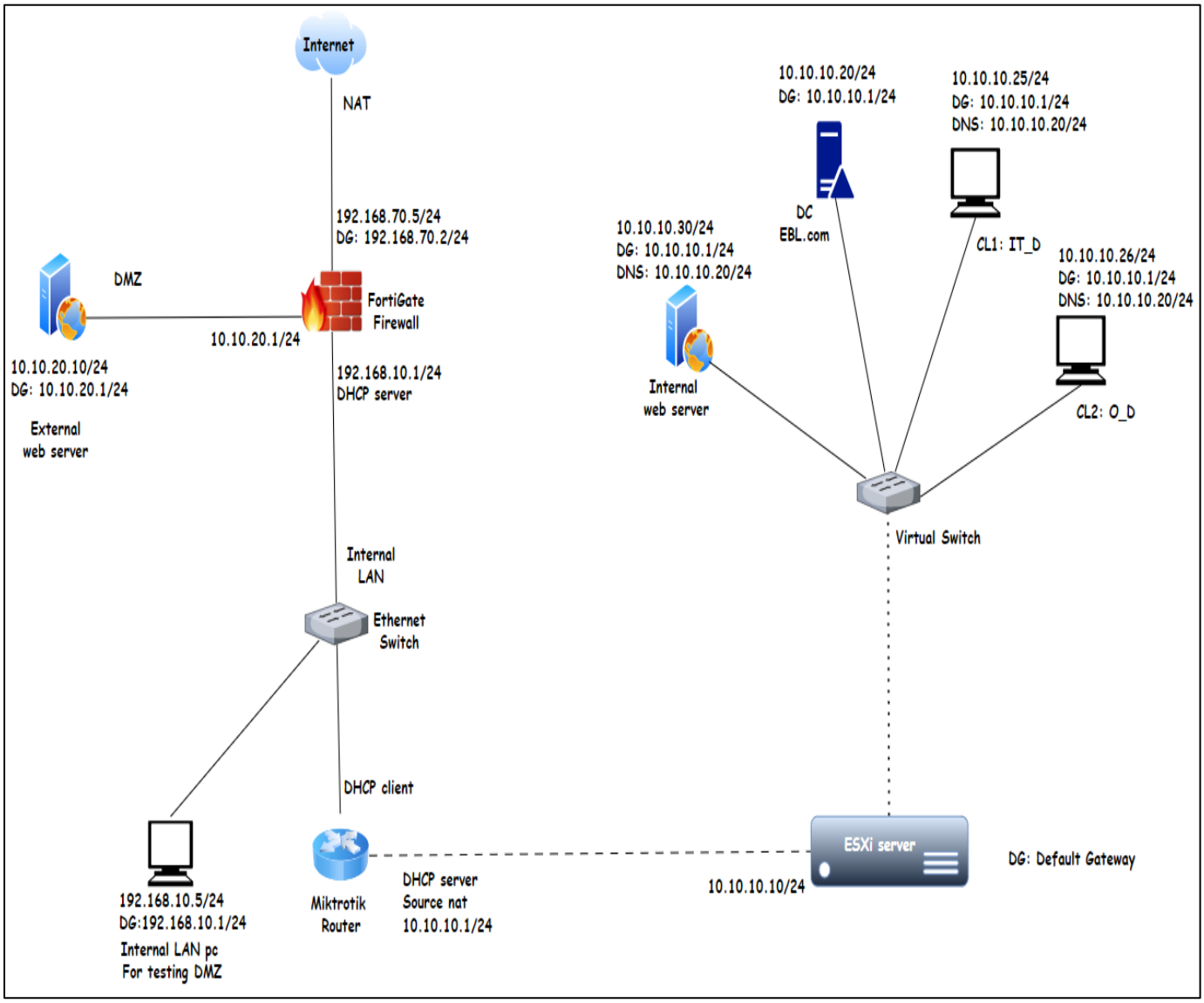


Figure 22 System architecture (logical topology)

3.6.3. System workflow

The system workflow outlines a secure network structure where an external user accesses a web server through the internet, with a FortiGate Firewall filtering traffic to allow only HTTP and HTTPS communication. This server sits within a DMZ, providing an additional security layer between external access and the internal network. A system administrator manages server operations and policies. Internally, another web server handles tasks like asset scanning and deploying packages using Lan sweeper and pdq deploy respectively. A domain controller facilitates authentication, account management, and policy control within the network, serving the needs of internal users who require authenticated access to various network resources. This setup effectively segregates external web traffic from internal network operations, bolstering security and control.

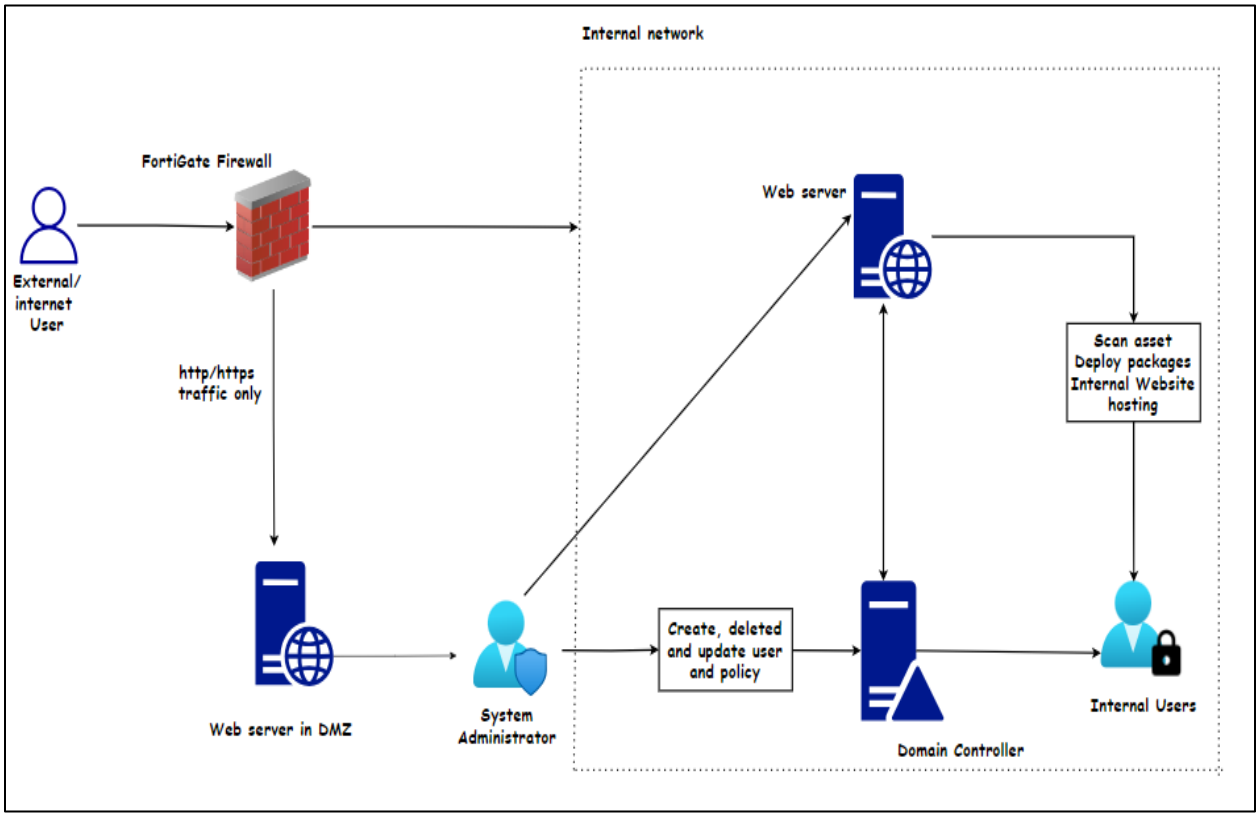


Figure 23 System Workflow

3.6.4. Active directory users and partitions

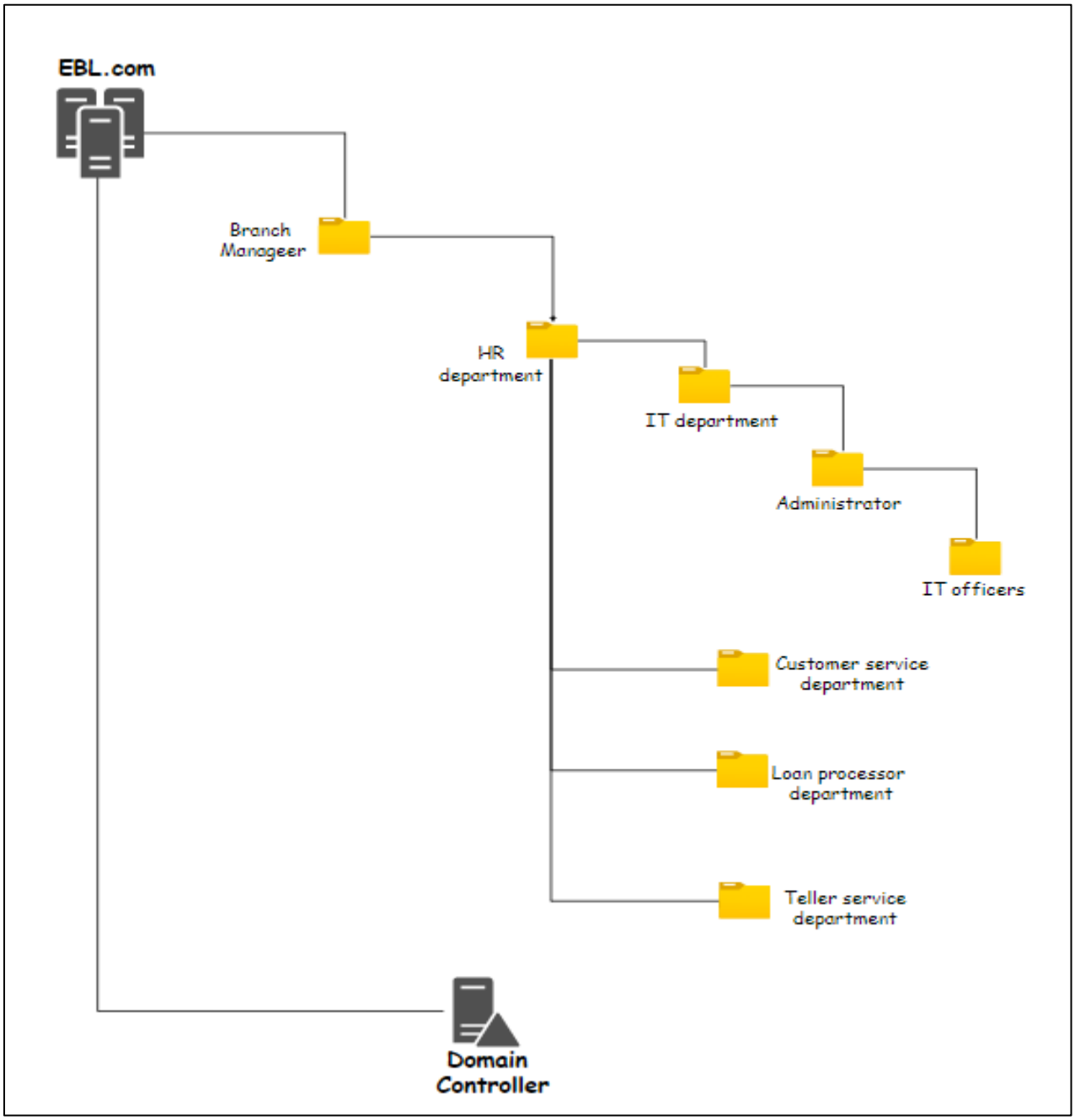
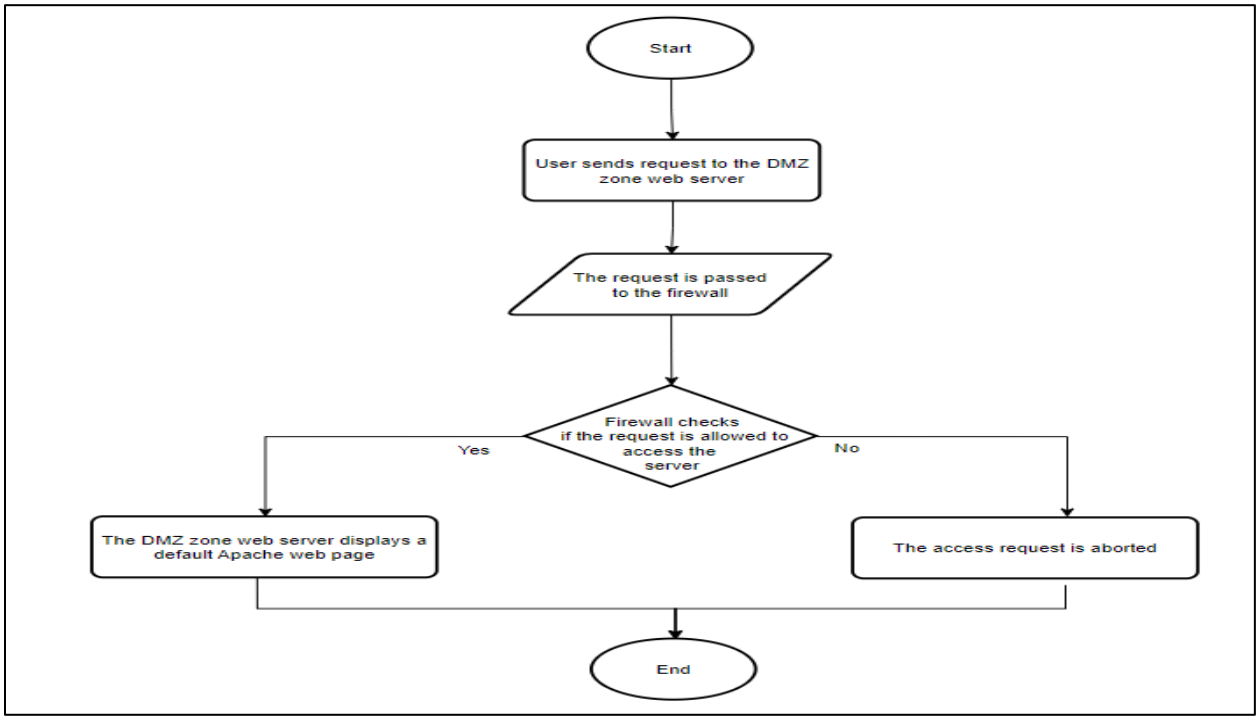
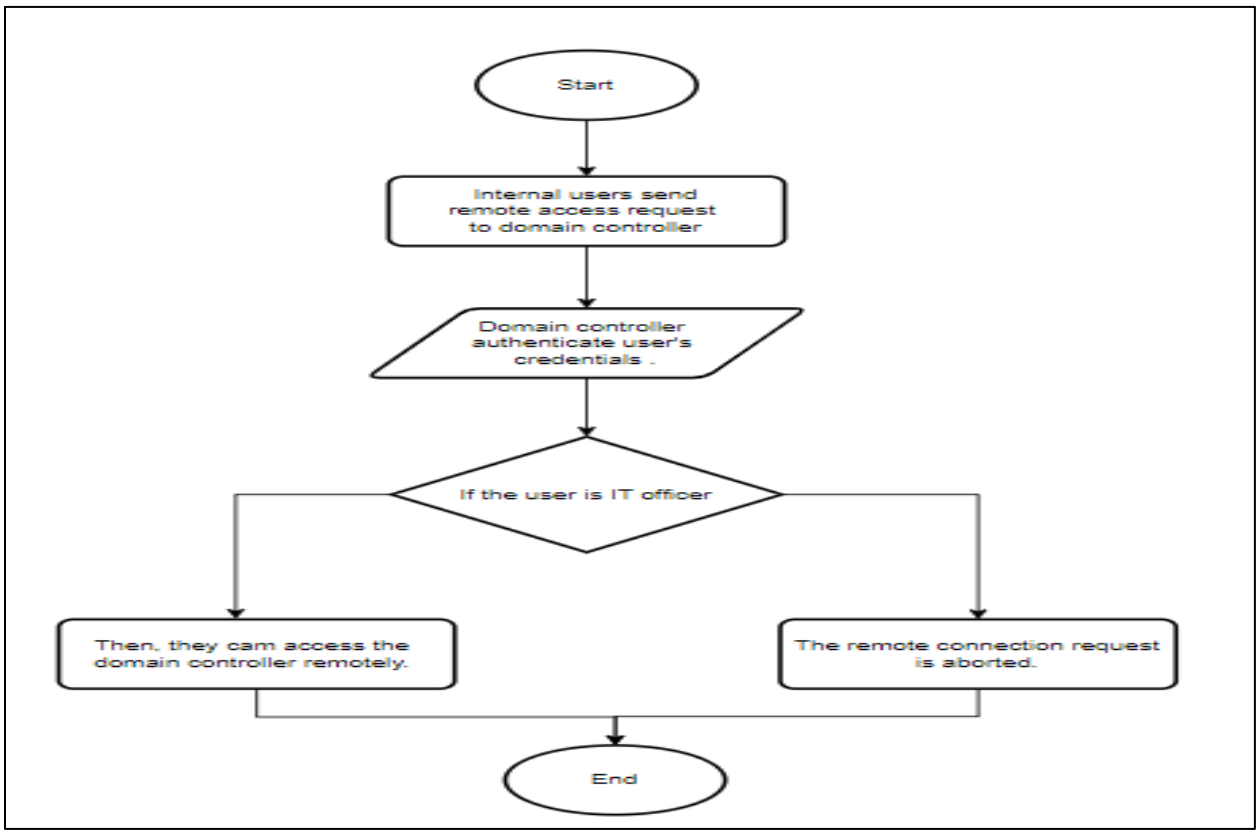


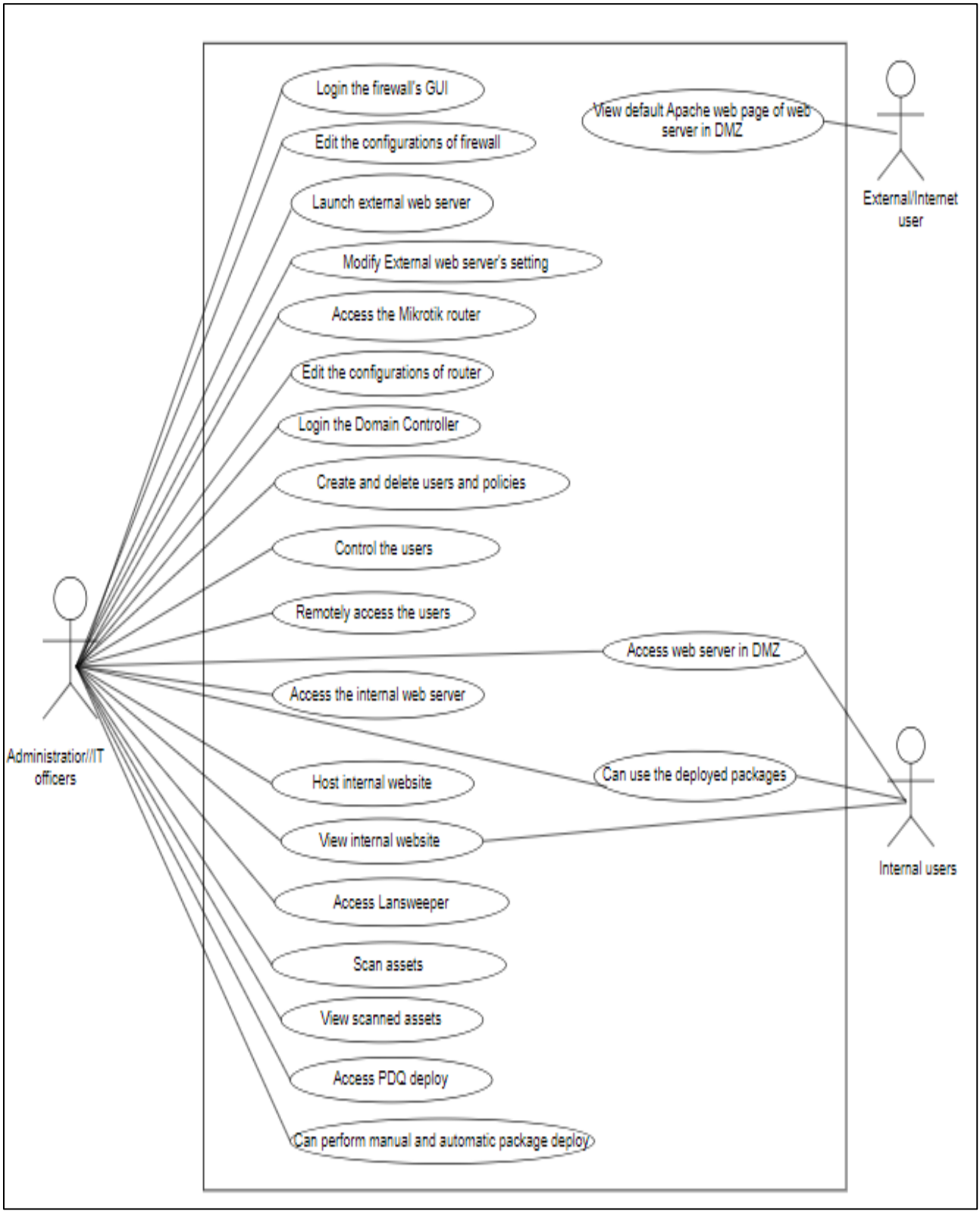
Figure 24 Active directory users and partitions.

3.6.5. Flow chart of the system





3.6.6. User case diagram



3.7. Implementation

The project is developed and implemented using different tools and methods that assist in the process. These tools and processes are used to support the system's development and implementation. The implementation is thoroughly demonstrated by showing screenshots to describe the utilized software and technologies.

3.7.1. GNS3 and GNS3 VM configuration

GNS3 is an open-source network simulation software that allow to design, configure, and test complex network topologies in a virtual environment. GNS3 VM is a virtual machine that acts as a separate additional server and can be added on gns3. In this project, GNS3 has been properly configured for creating a network topology and GNS3 VM has been configured as an additional server that provides internet to the cloud node of the topology.

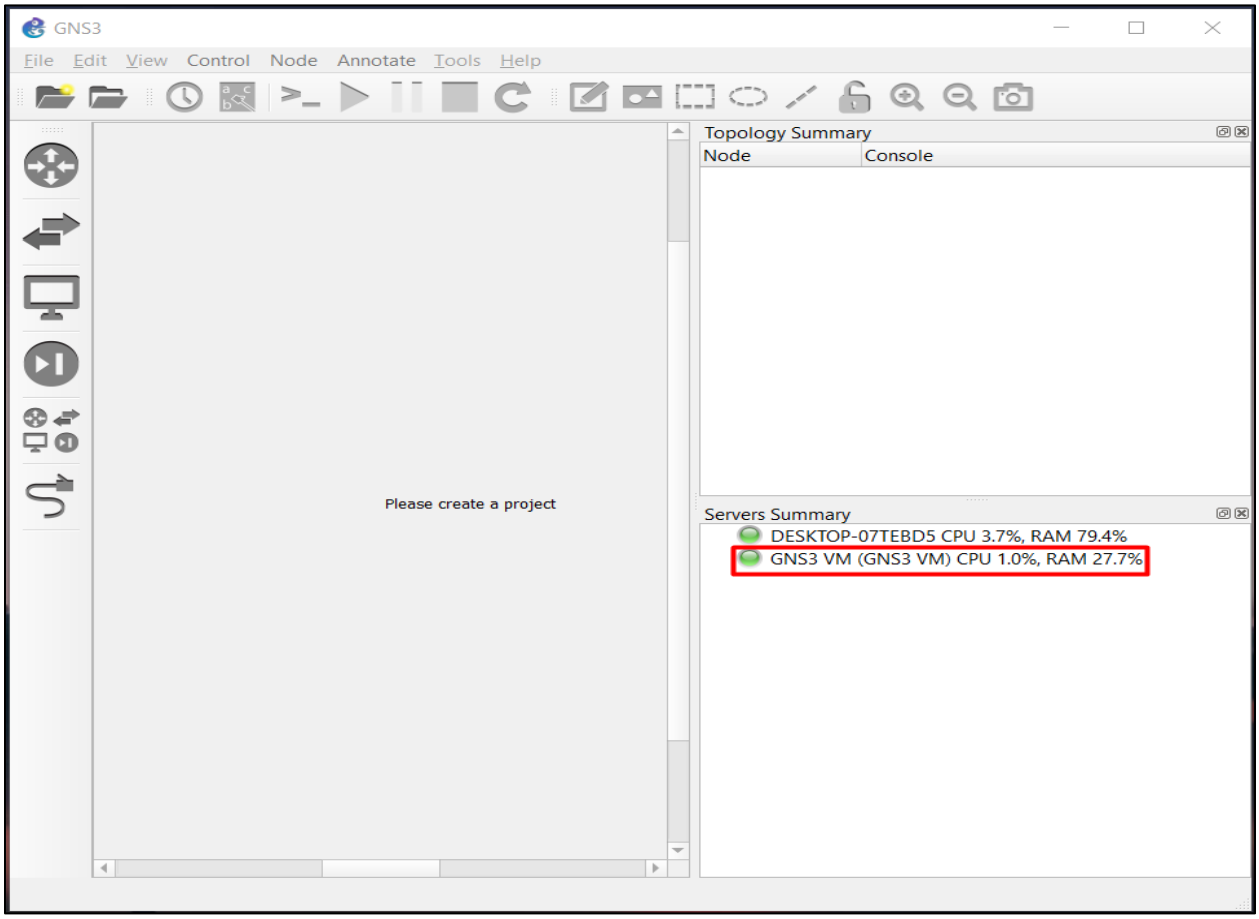


Figure 25 GNS3 and GNS3 VM configuration.

3.7.2. Firewall configuration

In this project, FortiGate Firewall 6.0.0.0 appliance is used. The firewall has been configured to create a DMZ zone for external web server. The http and https services of web server in the DMZ is accessible by both external/ internet users as well as internal users. The external users can access the http and https services only, thus restricting the limits to the internal network. For the DMZ configuration, two virtual IP were created, which further on followed by DMZ policies. The DHCP server is enabled on the interface connecting the internal network. Moreover, a policy allowing internet service to internal network has been also added in firewall.

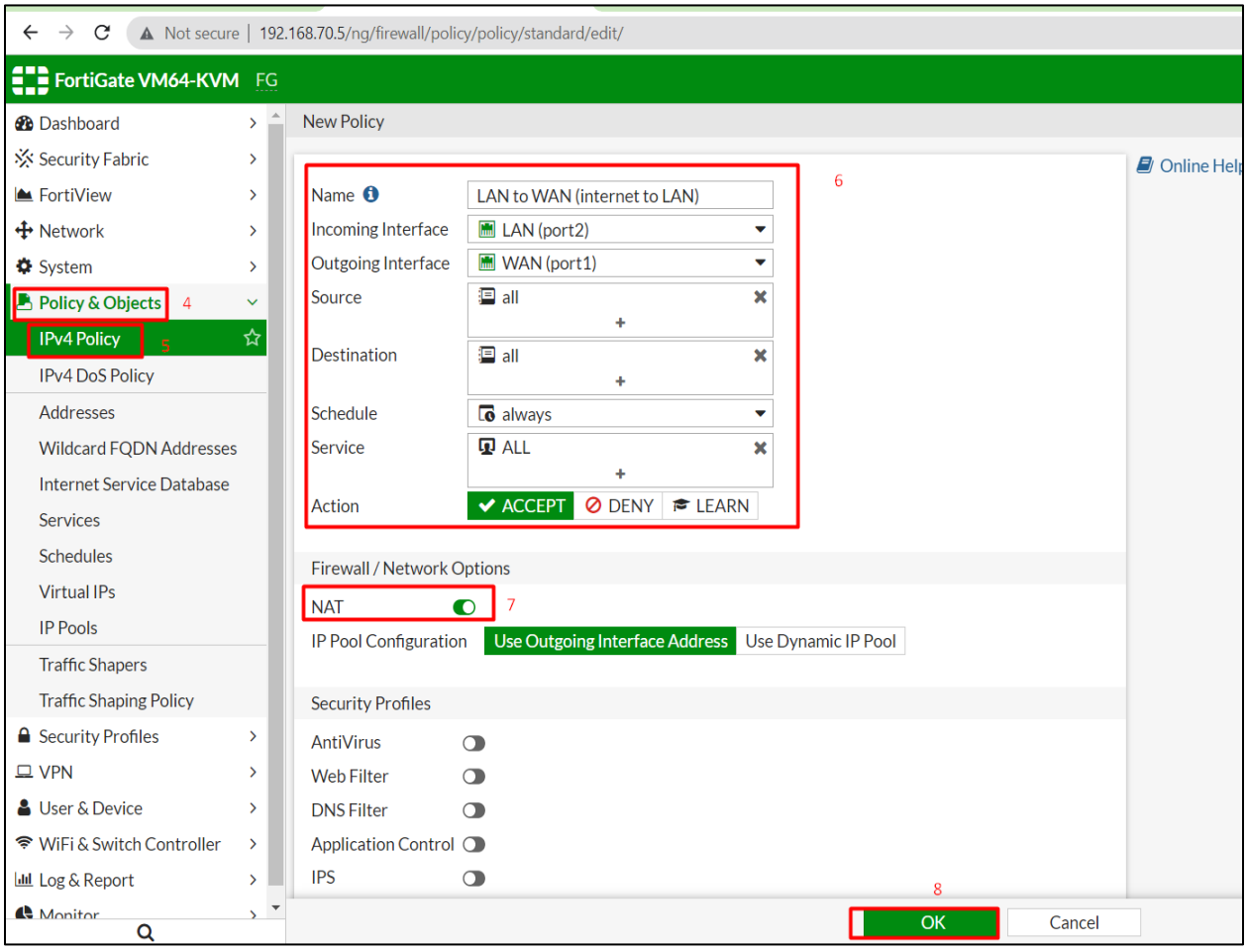


Figure 26 Firewall policy to allow internet in internal Network.

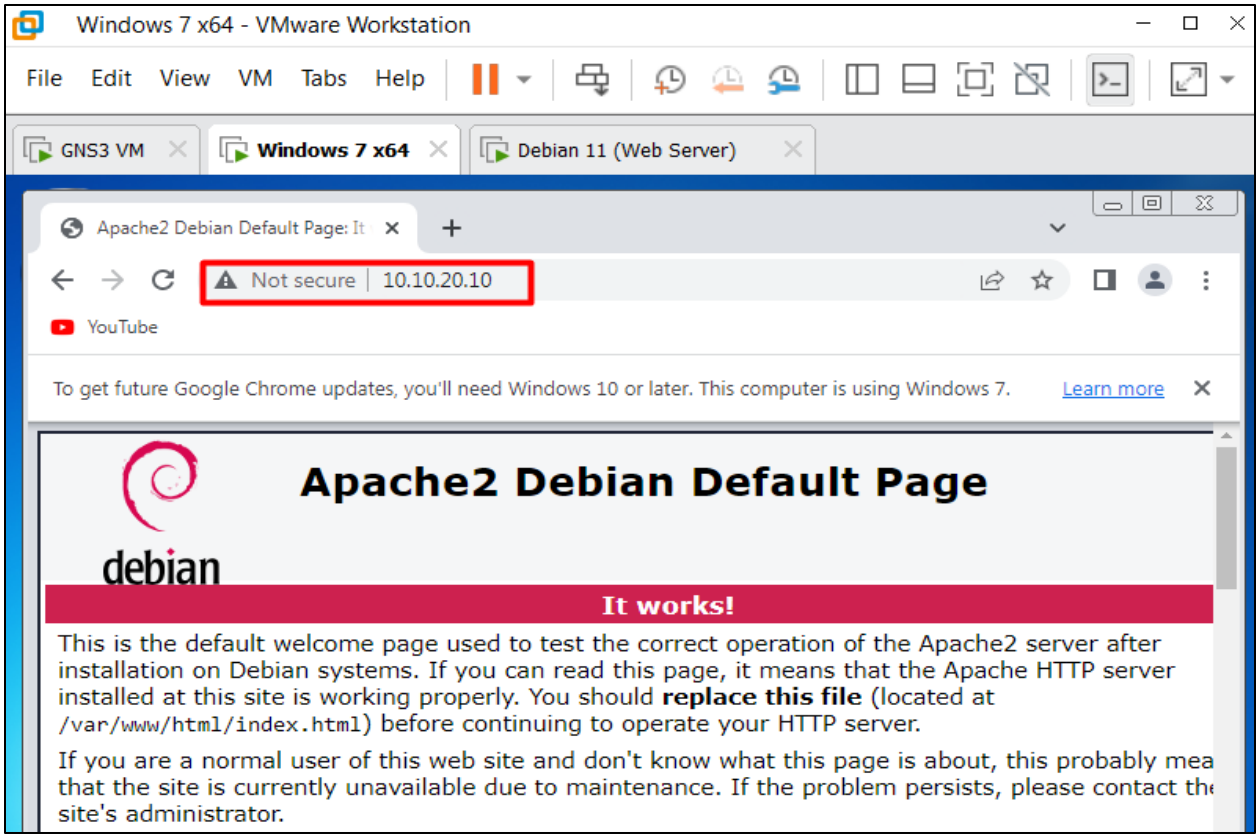


Figure 27 Web server in DMZ is accessible by internal users.

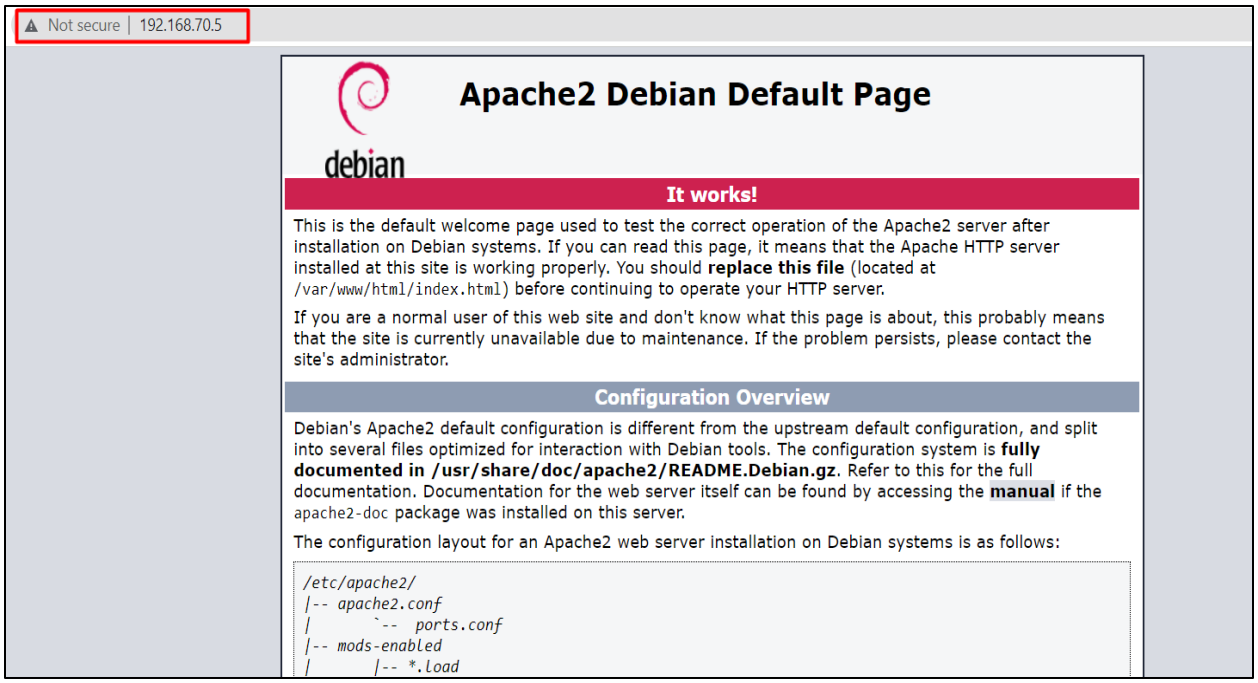


Figure 28 Web server in DMZ accessible by external/internet users.

3.7.3. External web server configuration

A web server is a server that delivers web pages or web applications to the clients over internet or an intranet. For the external web server configuration, the Debian 11 Linux is used. It is the latest stable release of the Debian Operating System and is a free-opensource Linux distribution (Debian.org, 2023). The web apache2 is installed for providing web services on this Linux. Moreover, a static IP address 10.10.20.10/24 is setup following the IP address of firewall's DMZ zone default gateway interface.

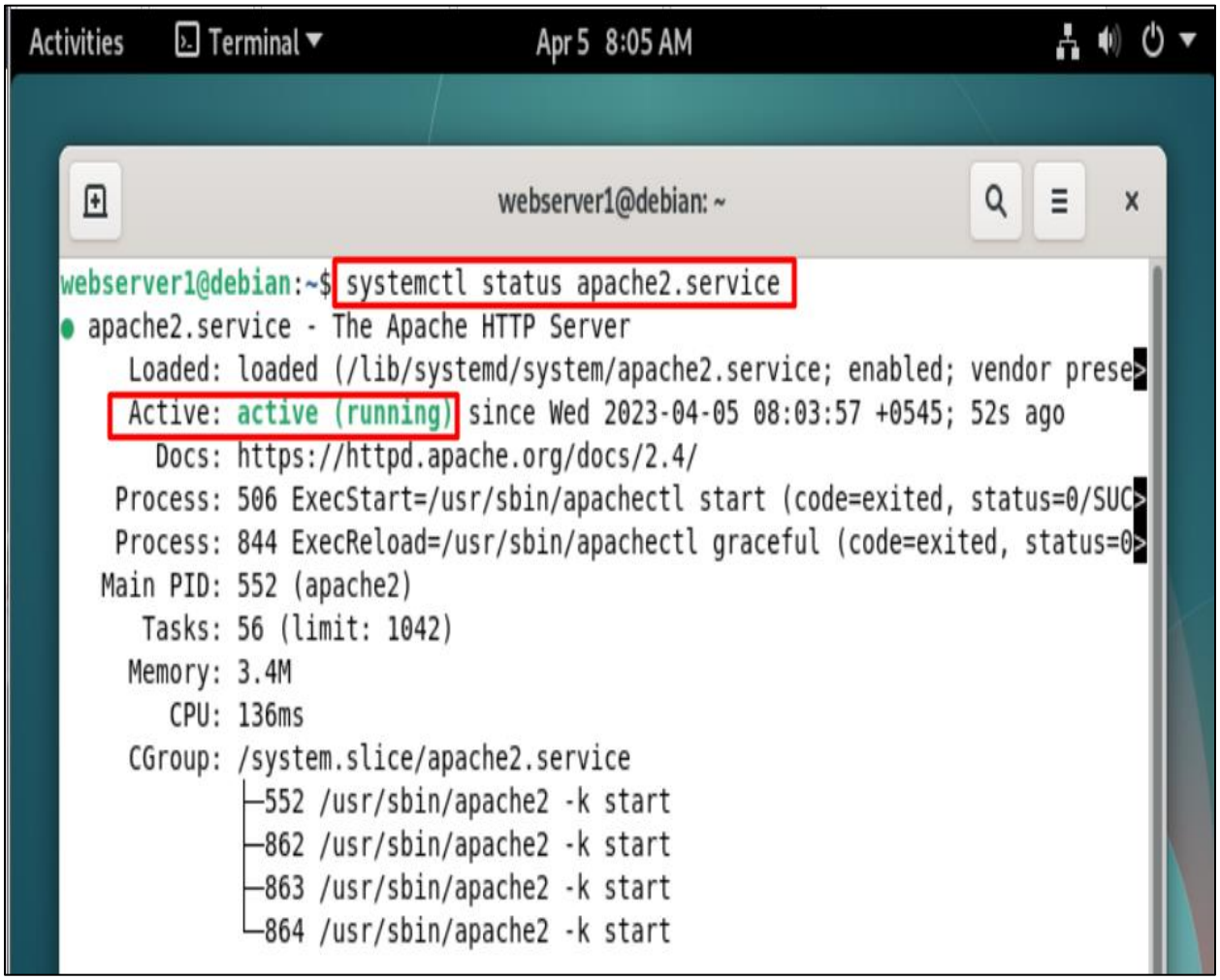


Figure 29 The web services actively running in Debian 11.

3.7.3. Miktrotik router configuration

In this project Miktrotik router has been configured for connecting the VMware ESXi to the GNS3 network topology because the VMware ESXi cannot be kept as a node in GNS3 user interface. For this configuration, the router is connected to the firewall and DHCP client is enabled on the interface of the router that is connected with the firewall. Then an IP address 10.10.10.1/24 is assigned on the Ether2 interface and DHCP server is enabled. Additionally, the source Nat is enabled in the 10.10.10.0/24 network. Thus, allowing the proper internet connection flow in the ESXi server. The IP address of the ESXi is set i.e., 10.10.10.10./24.

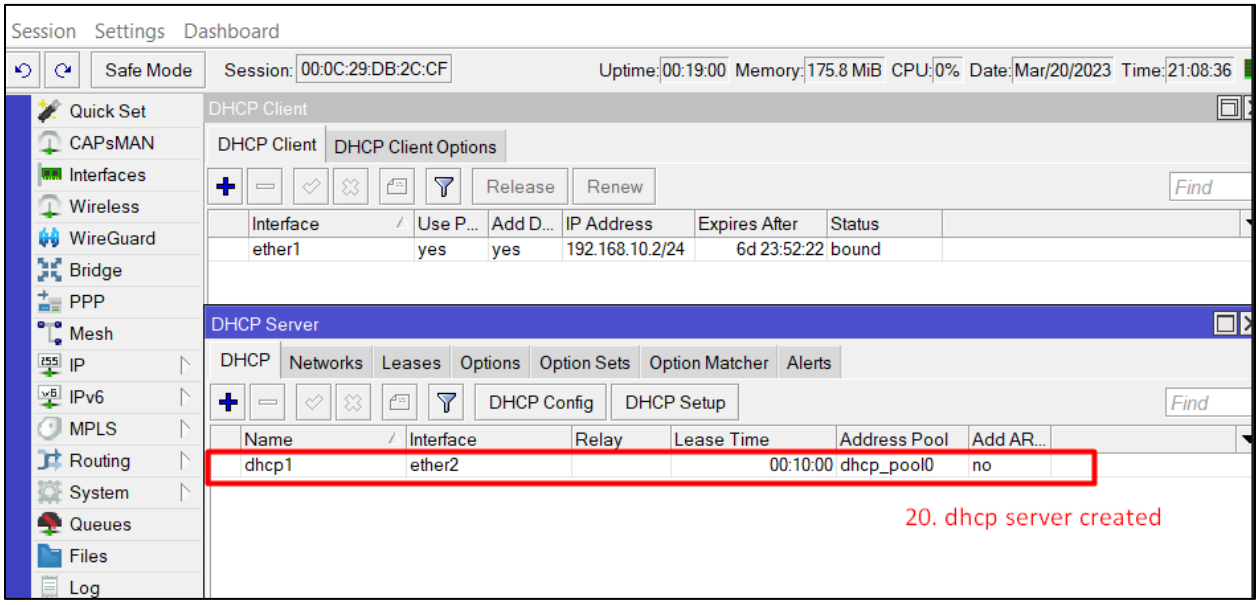


Figure 30 DHCP server configuration on Ether2.

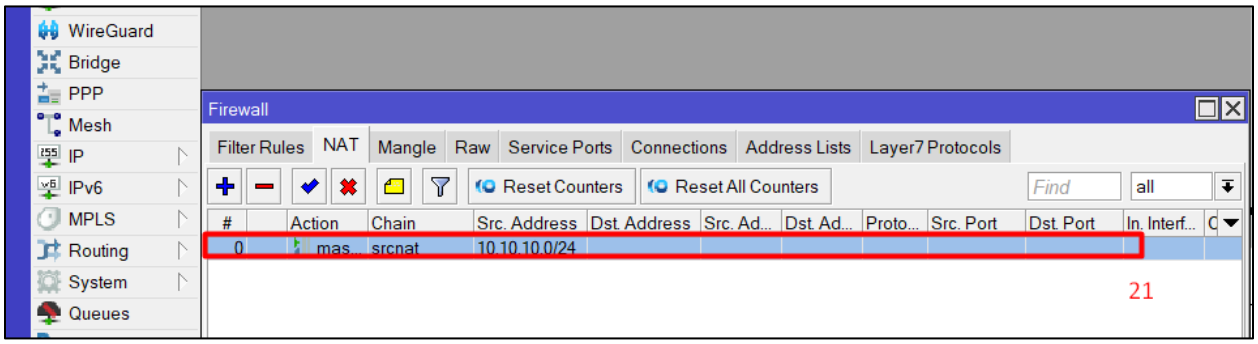


Figure 31 Source NAT configured for 10.10.10.0/244 network.

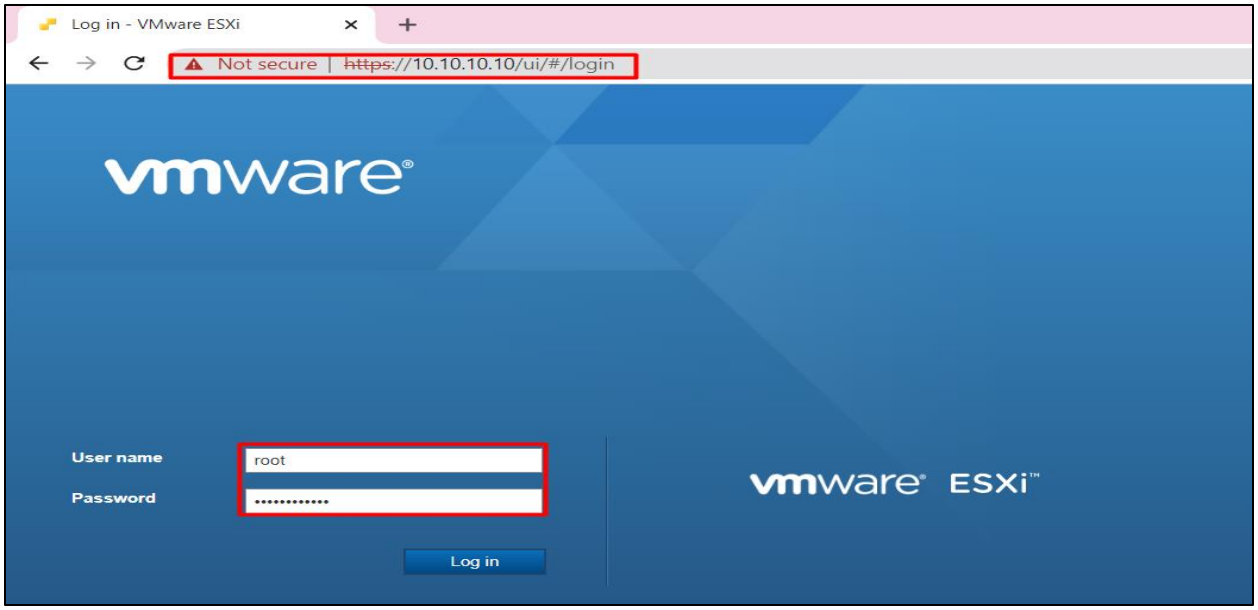


Figure 32 Accessing VMware ESXi GUI successfully.

3.7.4. VMware ESXi configuration

The VMware ESXi is a virtualization tool that allows virtual machines to run on a single server, each with their own operating system. Regarding this project, four VMs are configured on the VMware ESXi 7 i.e., domain controller, internal web server and two windows clients. All the VMs are in the same network i.e., 10.10.10.0/24.

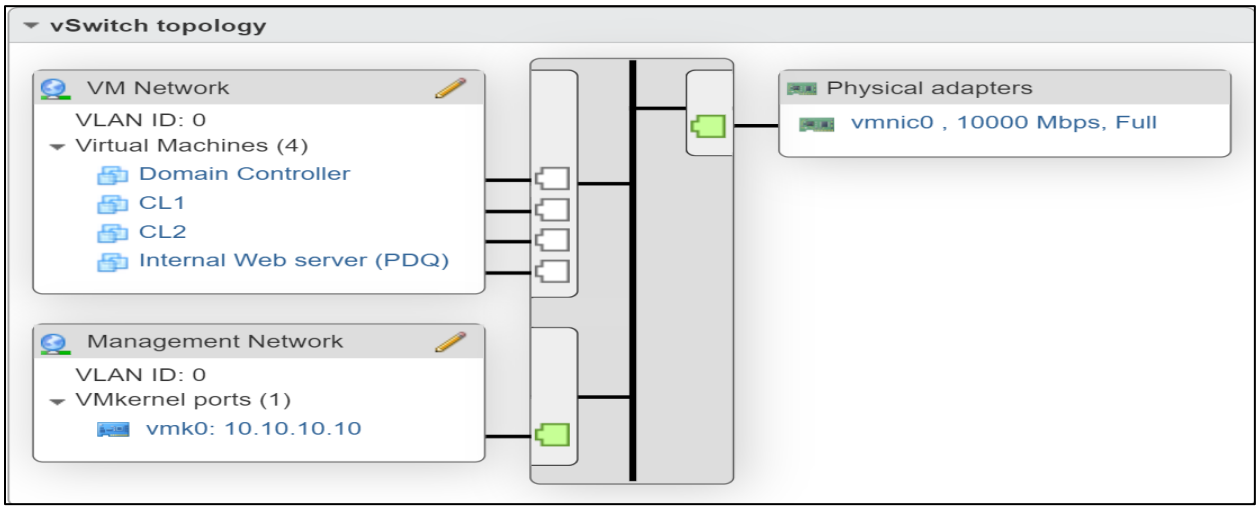


Figure 33 VMware ESXi configuration.

3.7.5. Domain controller configuration

The windows 2019 server has been configured as a domain controller. In order to configure the domain controller, the windows 2019 server has been promoted to DC using ADDS (Active Directory Domain Services) role. Then a new forest EBL.com is created and under this forest the internal web server, CL1 and CL2 has been added. Then, users for different department such as IT, HR etc., has been created.

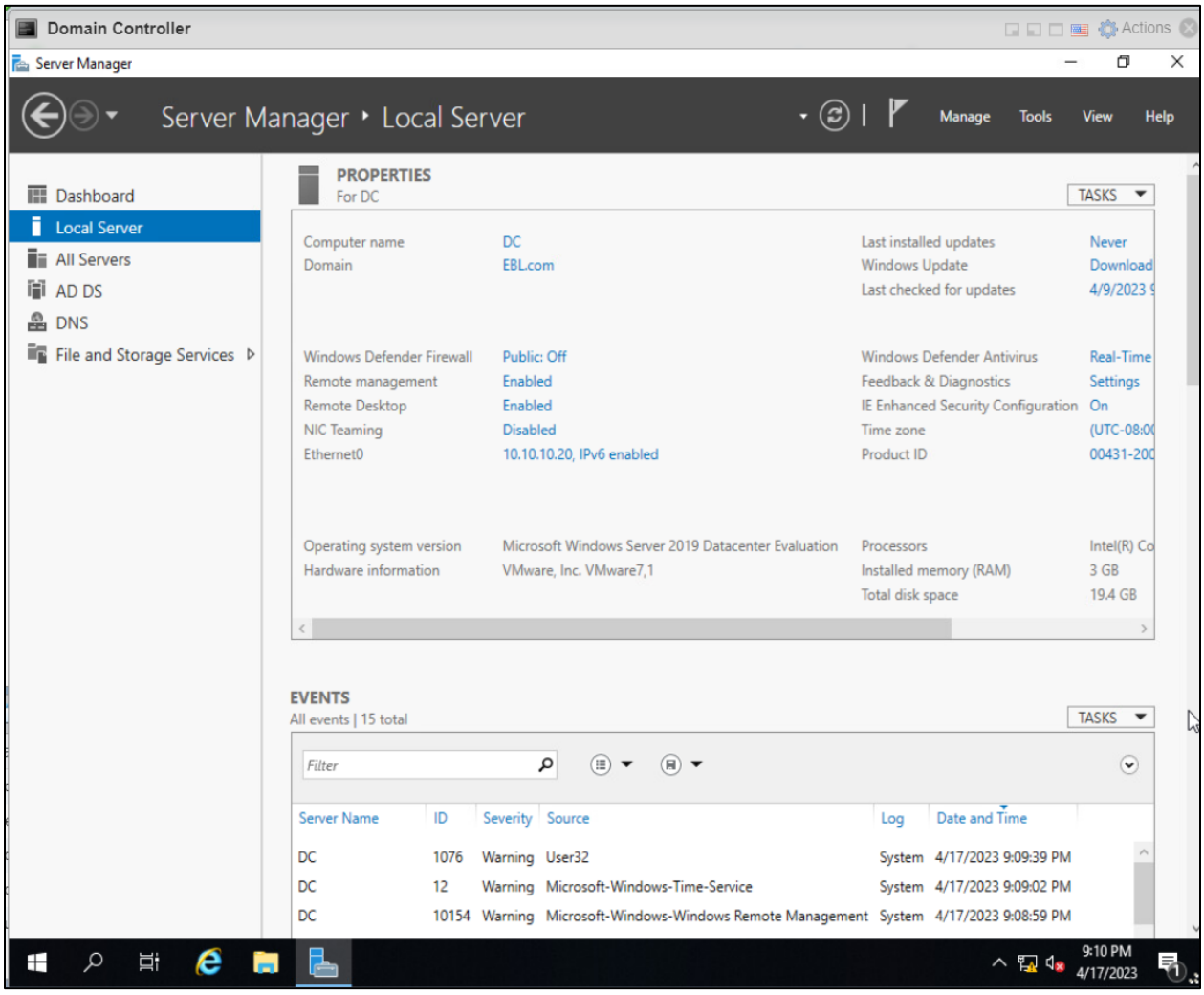


Figure 34 Promoted to domain controller,

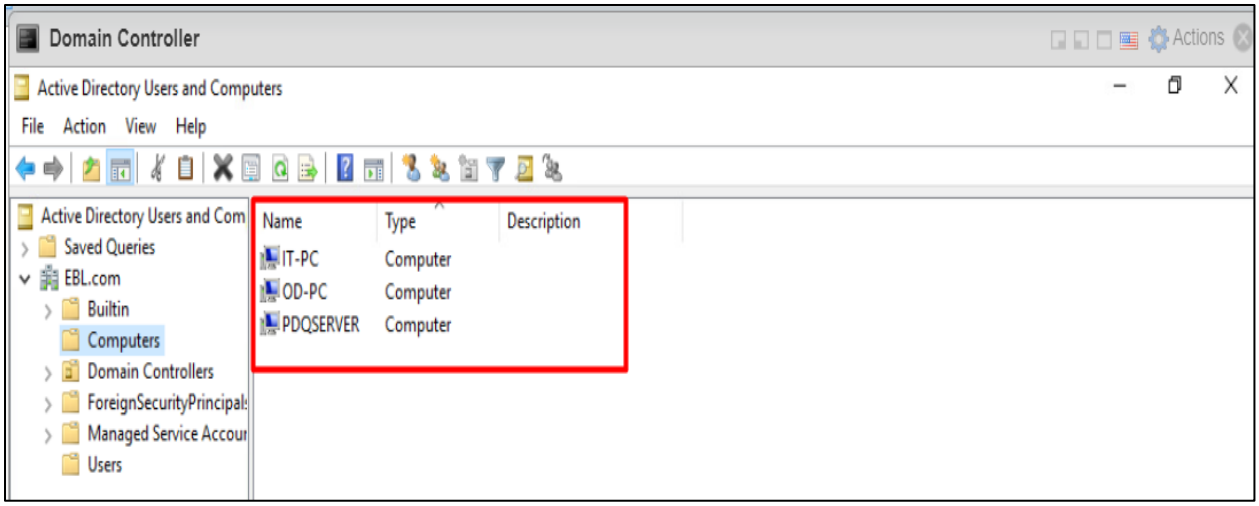


Figure 35 Added computers under EBL.com domain.

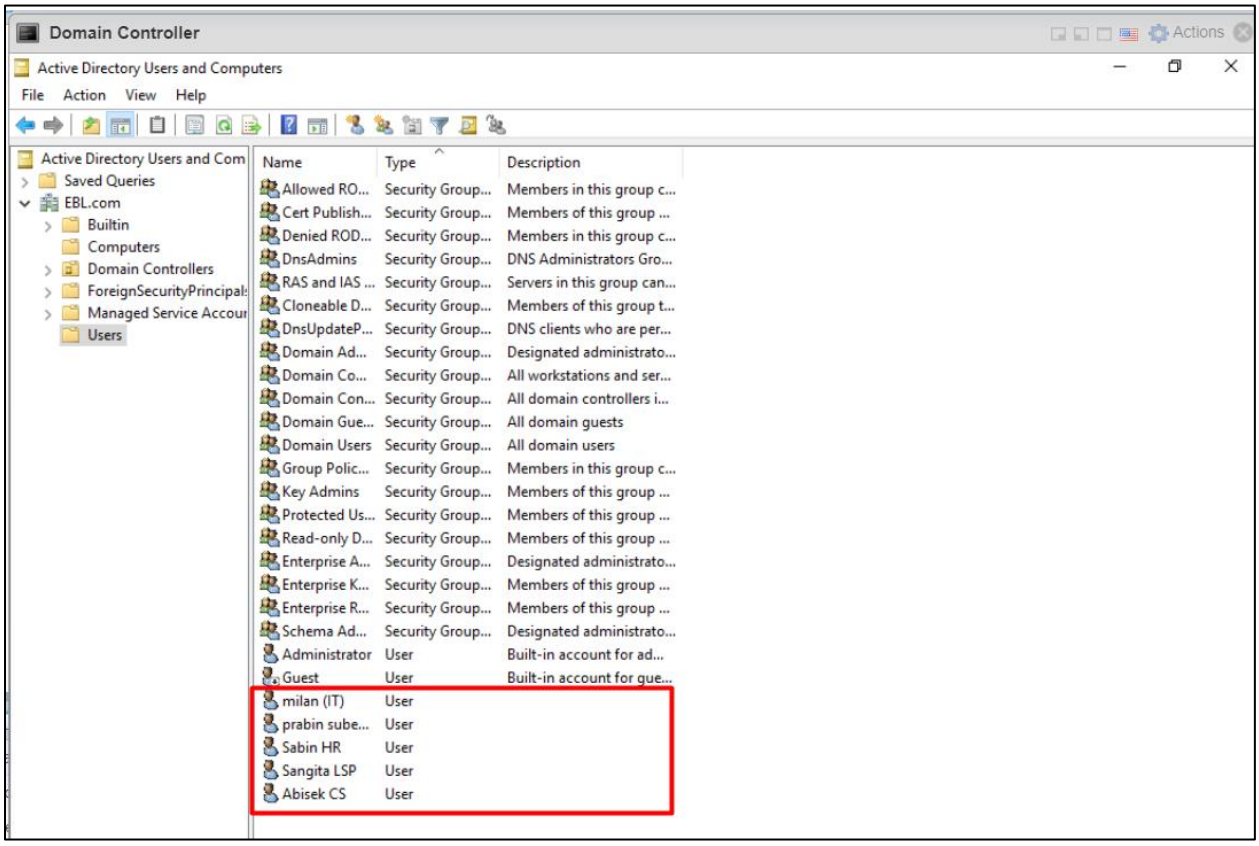


Figure 36 Added users under EBL.com domain.

3.7.5. Internal web server configuration

The internal web server is configured on windows 2022 server and kept under EBL.com domain. An internal website id hosted using the web server. Additionally, Lansweeper and PDQ deploy are implemented in the web server for enhancing the asset management and automated software package deployment and update package deployments.

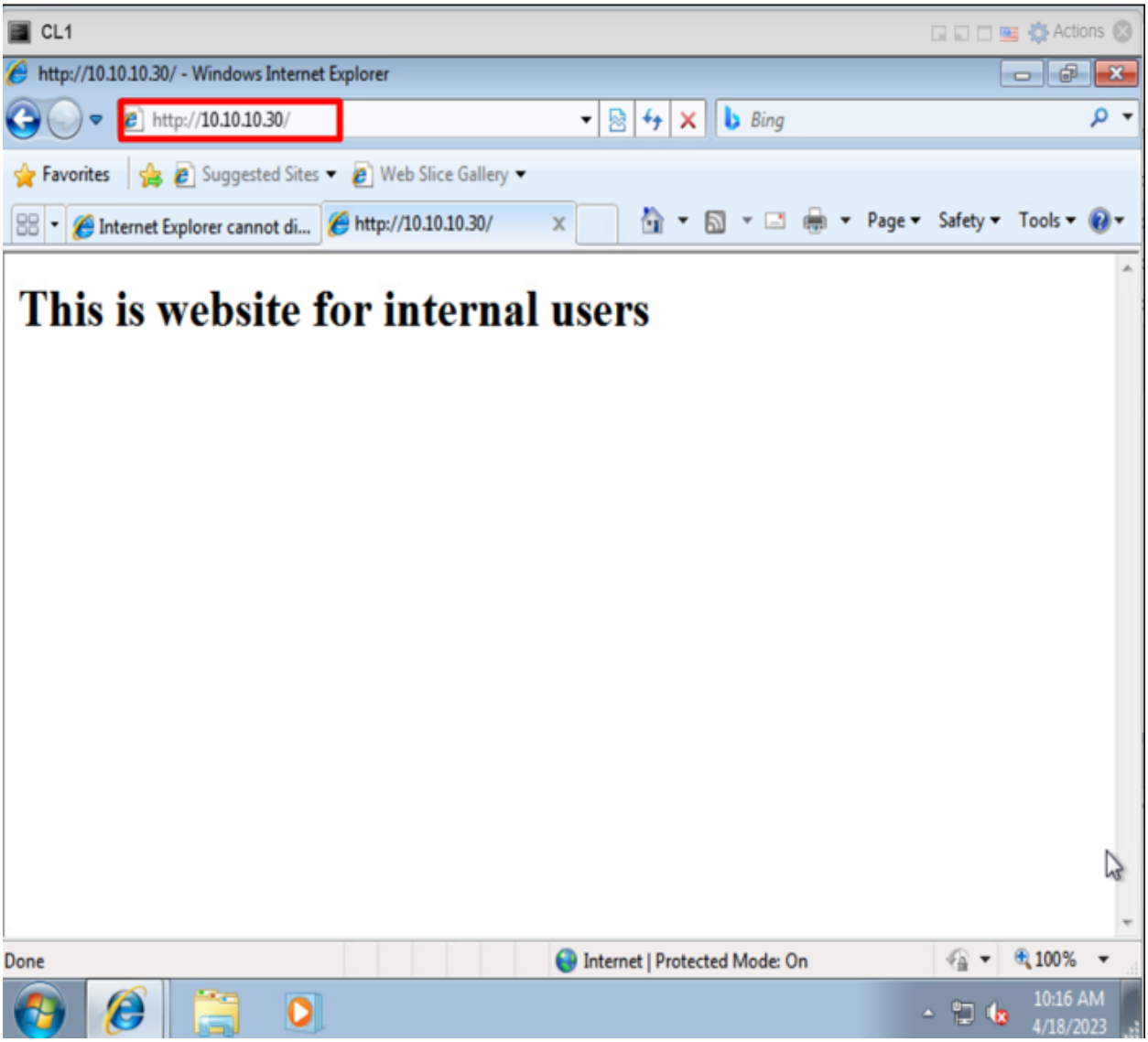


Figure 37 Website for internal users.

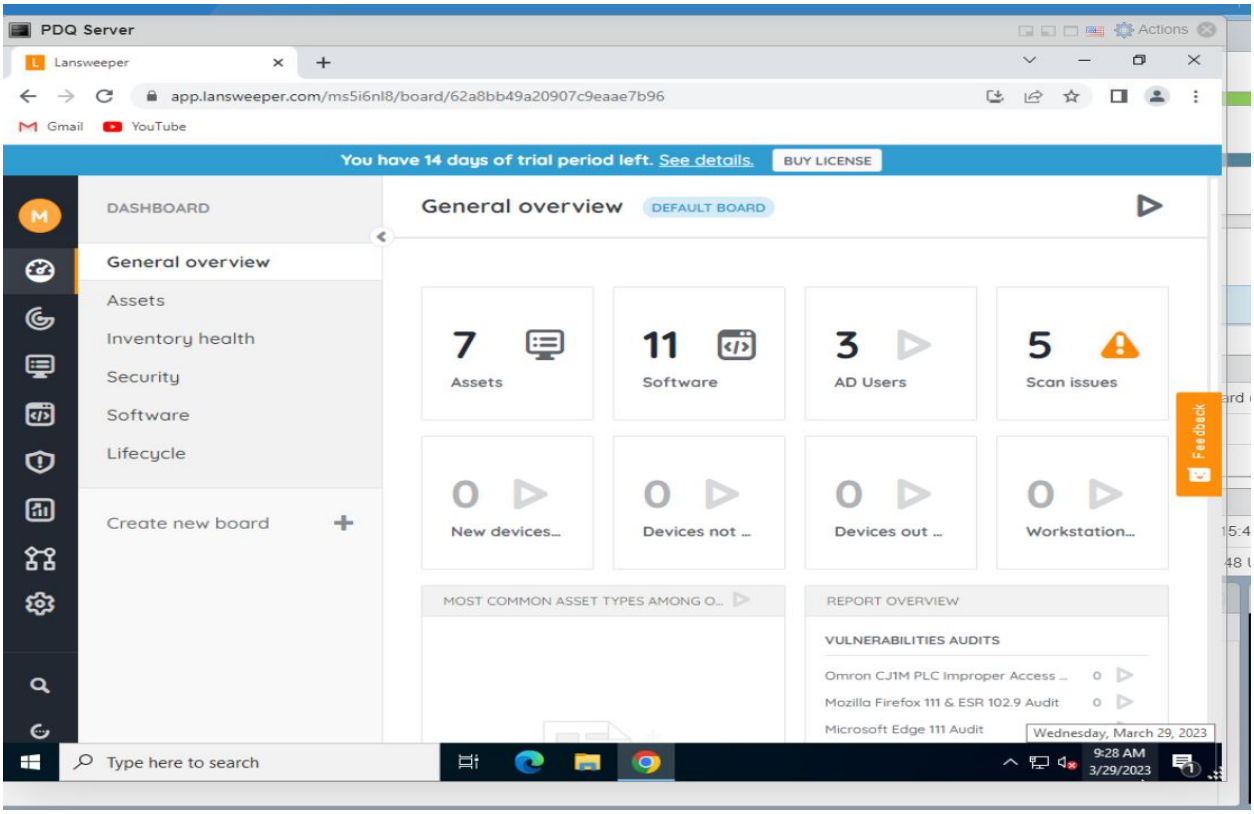


Figure 38 Lansweeper interface showing the scanned assets and software's.

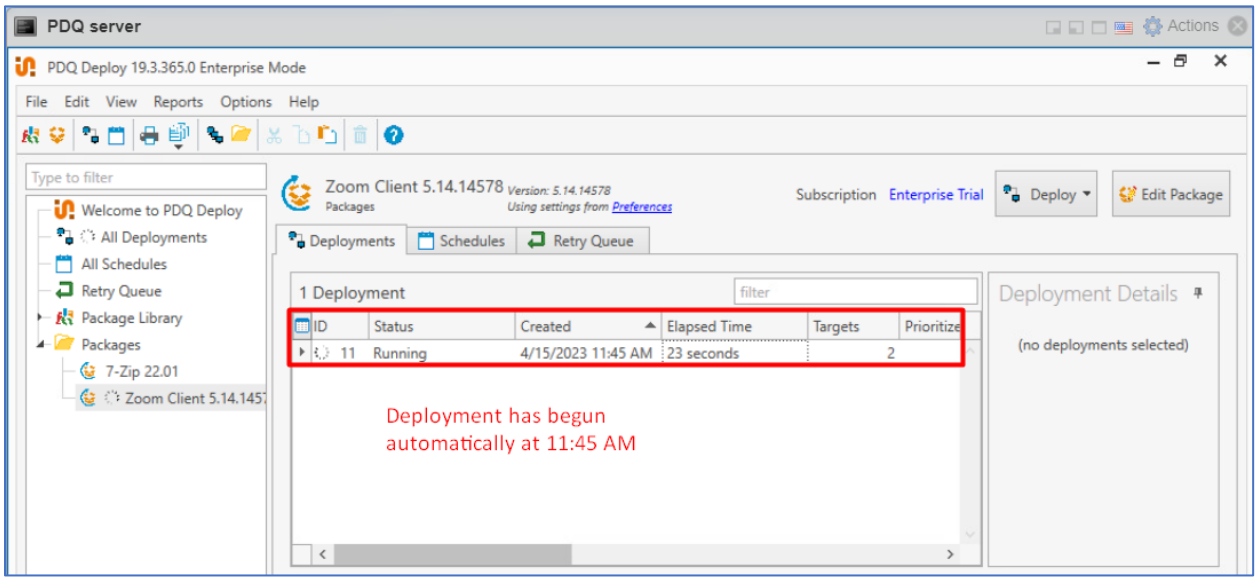


Figure 39 Automatic package deployment using PDQ deploy.

3.7.5. Windows clients configuration

For windows clients, two windows 7 enterprise version have been installed. One is for IT department and other is for all the department's users. The first PC can access the domain controller remotely and the other PC is used for other basic testing verification. Basically, These PCs are used as clients to verify performance like asset management and scanning, the internal website hosting, package deployments and remote access policies.

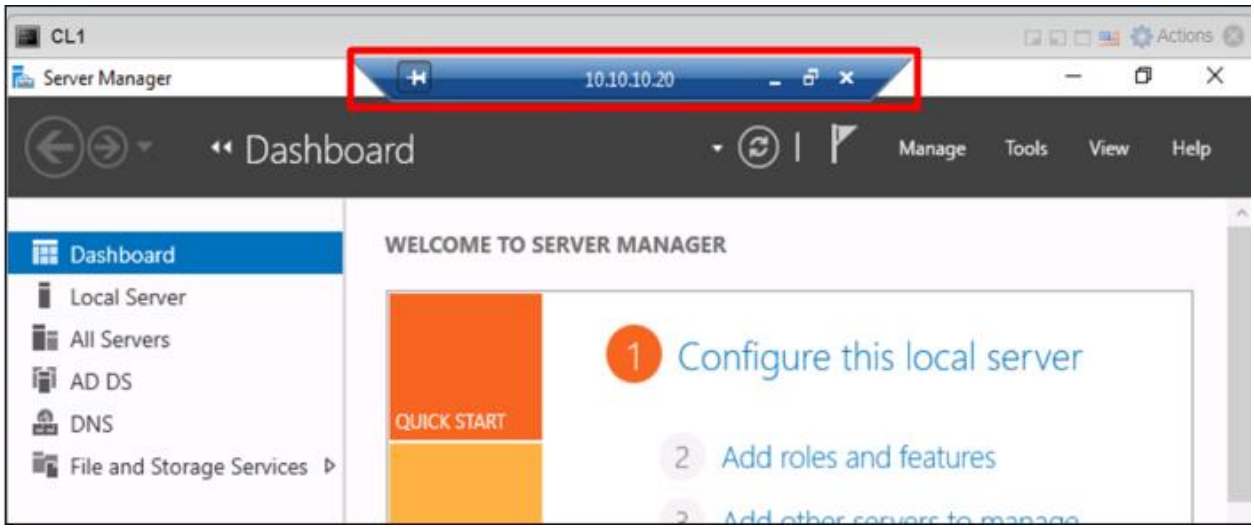


Figure 40 IT officers accessing DC remotely.

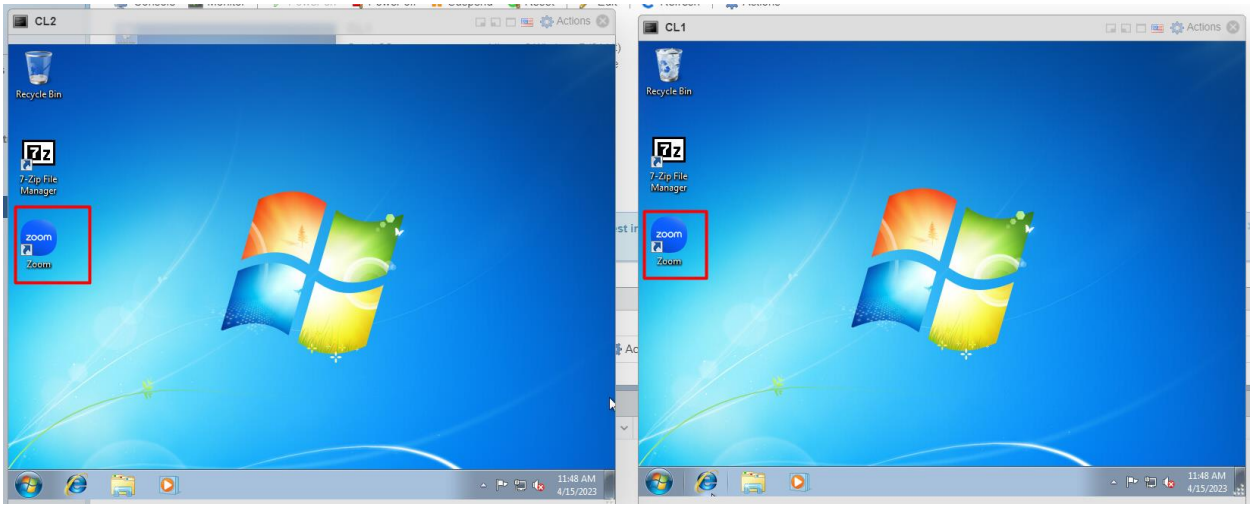


Figure 41 Verifying package deployments.

The detailed configuration of these devices is presented in section 8.4 Appendix D.

CHAPTER 4: TESTING AND ANALYSIS

4.1. Test plans

Basically, the test plans are designed by software/system tester to guarantee the quality, functionality and performance of the developed system. This project includes altogether eight test plans, which are listed below,

4.1.1. Unit testing

4.1.1.1 GNS3 VM test plan

Test Case	Objectives
1	To test whether the GNS3 VM server is successfully integrated and functional in GNS3 interface or not.
2	To test whether the gns3 VM server in providing internet connectivity or not.

Table 2 gns3 VM server test Plan

4.1.1.2 gns3 test plan

Test Case	Objectives
1	To test if the virtual adapter (VMnet) that connects the VMware workstation's VM in GNS3 is functioning properly or not.

Table 3 gns3 test plan

4.1.1.3 External Web server test Plan

Test Case	Objectives
1	To test whether the web server is installed in Debian 11 Linux or not.

Table 4 Debian Web server (in DMZ) test plan

4.1.1.4 FortiGate firewall test plan

Test case	Objectives
1	To test whether the FortiGate firewall is properly installed or not.
2	To test if the firewall's GUI is accessible or not.
3	To test the connectivity between the internal LAN and firewall.
4	To test the internet connectivity in the internal network.
5	To test the configuration between external web server and firewall for implementing DMZ.

Table 5 FortiGate firewall test plan

4.1.1.5. Miktrotik Router OS test Plan

Test Case	Objectives
1	To test whether there is any loss of internet connectivity on the interfaces or not.
2	To test whether the router can communicate with all the VMs configured inside ESXi or not.

Table 4 Miktrotik Router OS test Plan

4.1.1.6. VMware ESXi test plan

Test Case	Objectives
1	To test whether the VMware ESXi is properly installed or not.
2	To test whether the increment of the datastore is successful or not.

Table 5 VMware ESXi test plan

4.1.1.7. Domain controller test plan

Test Case	Objectives
1	To test whether the DNS server is successfully installed and configured or not.
2	To test whether the computers are added in the domain controller or not.

Table 6 Domain Controller test plan

4.1.1.8. Internal web server test plan

Test case	Objectives
LAN sweeper test plan	
1	To test whether the LAN sweeper is installed properly or not.
2	To test whether Lansweeper meet the perquisites to begin scanning.
PDQ deploy test plan	
3	To test whether the pdq deploy is installed in enterprise mode or not.

Table 7 Internal server test plan

4.1.2. System testing

4.1.2.1. Demilitarized Zone test plan

Test Case	Objectives
1	To test whether the web server in DMZ is accessible by the external users or not.
2	To test whether the web server in DMZ is accessible by internal users or not.

Table 8 DMZ test plan

4.1.2.2. Remote access policies test plan.

Test Case	Objectives
3	To test whether the domain controller can remotely access all the users and computer or not.
4	To test whether the IT officers can remotely access the domain controller or not.
5	To test if the other department's users can remotely access the Domain Controller or not.

Table 9 Remote access policies test plan

4.1.2.3. Internal website test plan.

Test Case	Objectives
1	To test whether the internal website is hosted or not.

Table 10 Internal website test plan

4.1.2.3. Asset management test plan.

Test Case	Objectives
6	To test whether the LAN sweeper is scanning the assets present in the network or not.
7	To test whether the LAN sweeper is showing any credentials issue or not.

Table 11 Asset management test plan

4.1.2.4. Software package deployment test plan.

Test Case	Objectives
8	To test whether the package is added for deployment or not.
9	To test whether the manual package deployment is successful or not
10	To test the scheduled and triggered package deployment is successful or not.
11	To test whether the deployed package is functional or not.

Table 12 Software package deployment test plan.

4.2. Test Cases

The cases are performed in accordance with the test plans that are presented above. The unit and system testing are presented below ensuring the error free system,

4.2.1. Unit testing

4.2.1.1. GNS3 VM test cases.

Test case 1	
Objective	To test whether the GNS3 VM server is successfully integrated in GNS3 or not.
Action	Install GNS3 VM in VMware workstation and enable the GNS3 VM from the preferences.
Expected test Result	The GNS3 VM should start and function automatically upon launching the gns3.
Actual test result	The GNS3 VM started and functioned automatically upon launching the gns3.
Conclusion	Successfully done.

Table 13 GNS3 VM test case 1

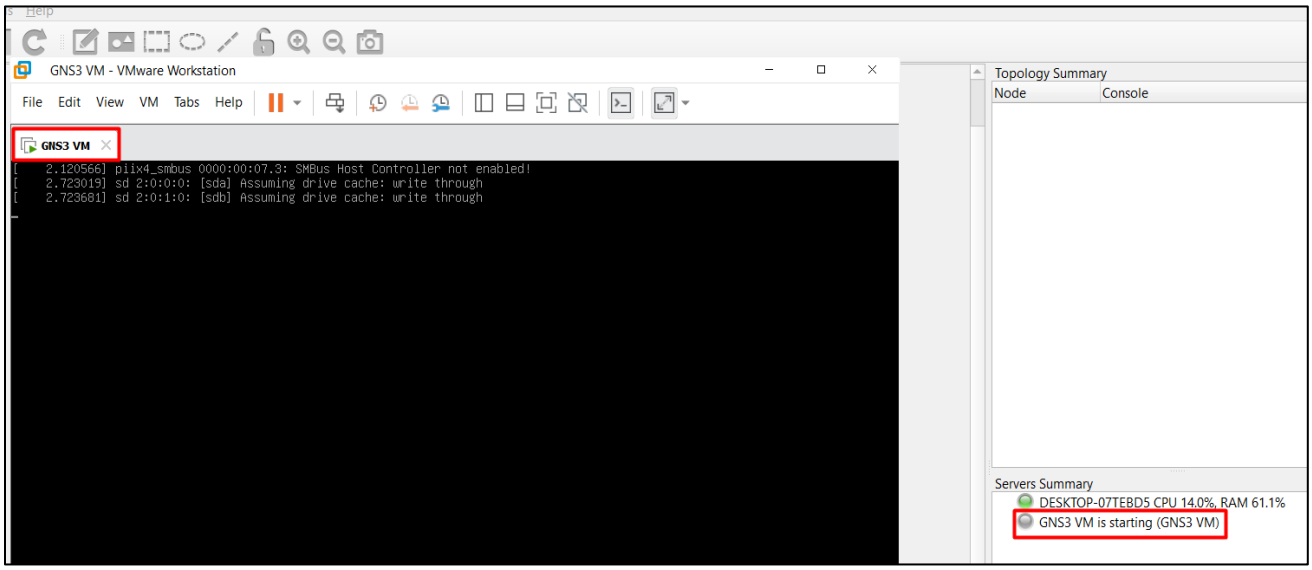


Figure 42 Test results: the gns3 VM started automatically upon launching the gns3.

Test case 2	
Objective	To test whether the gns3 VM server in providing internet connectivity or not.
Action	Access the GNS3 VM's GUI using its assigned IP address (192.168.70.4) or Ping the IP address using local PC's CLI.
Expected test Result	The GNS3 VM's GUI should be accessed, or the IP address should be pingable to provide internet to the gns3 appliances.
Actual test result	The GNS3 VM's GUI is accessed, and IP address is pingable through local PC.
Conclusion	Successfully done.

Table 14 GNS3 VM test case 2.

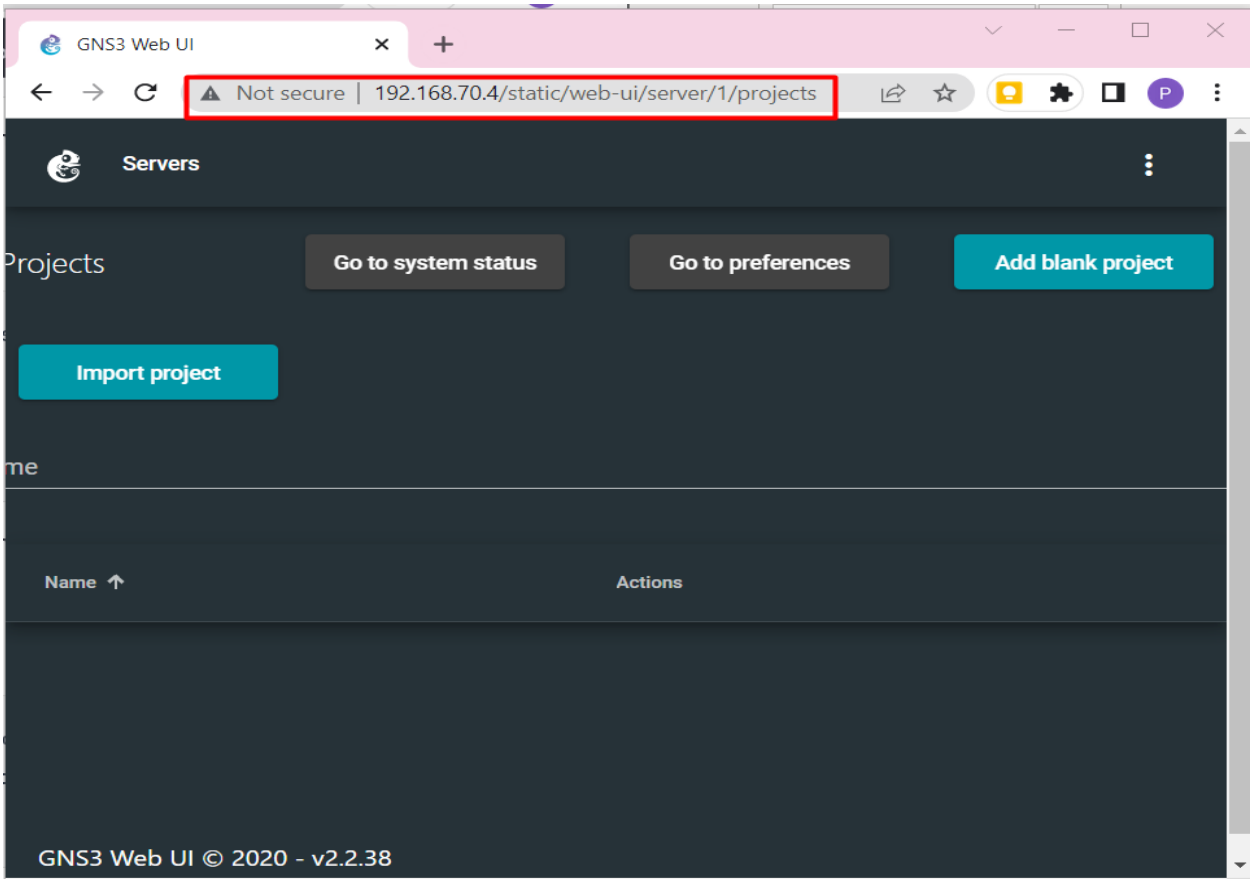


Figure 43 Test results: The GUI of GNS3 VM accessed successfully.

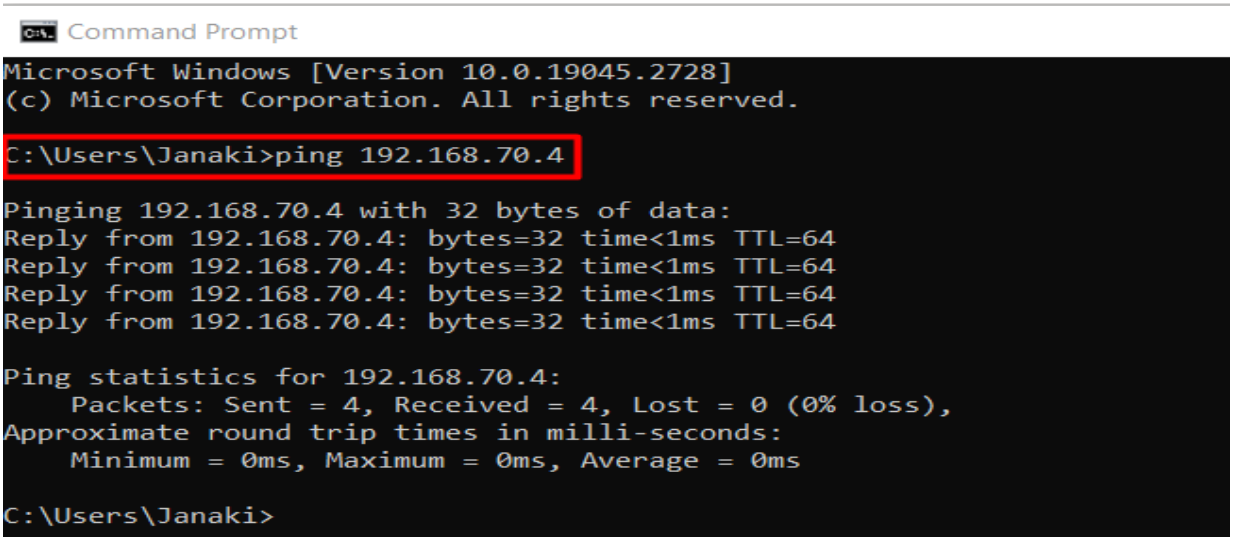


Figure 44 Test results: The IP address of GNS3 VM was pingable from local PC.

4.2.1.2. gns3 test case

Test case 1	
Objective	To test if the virtual adapter (VMnet) that connects the VMware workstation's VM in GNS3 is functioning properly or not.
Action	• Keep external web server (Debian 11) as a node in gns3. • Connect the node with firewall appliance and start.
Expected test Result	The VM node should start and run automatically.
Actual test result	The ethernet is not able to connect with VM node and was throwing an error message.
Error	No VMnet interface available between VMnet2 and VMnet19 for connection.
Correction	It was corrected by adding VMnet interface (Go to preferences> VMware> Network> configure)
Conclusion	Successfully done.

Table 15 GNS3 test case 2

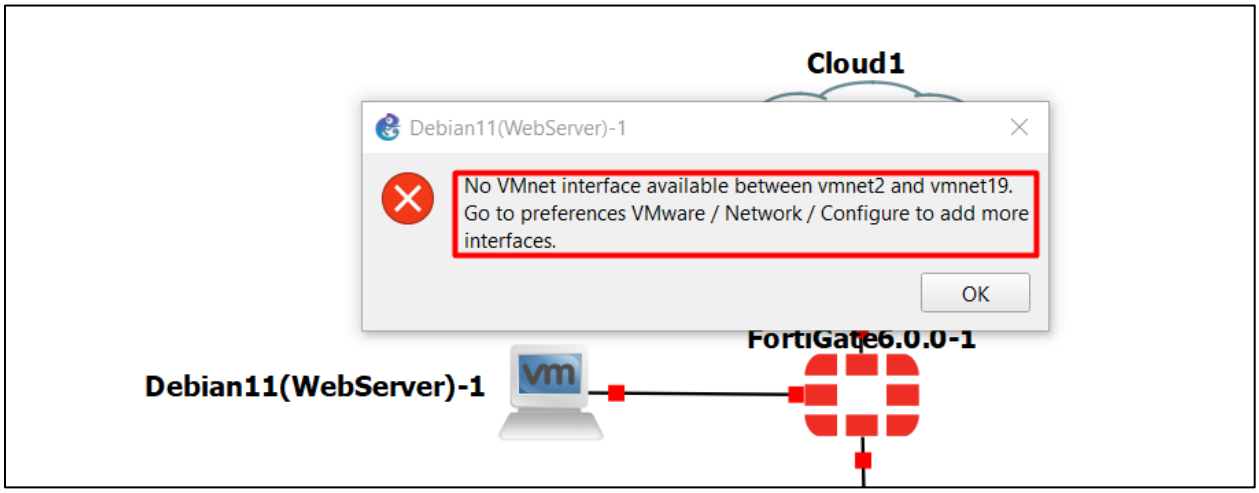


Figure 45 Error of GNS3 test case 1

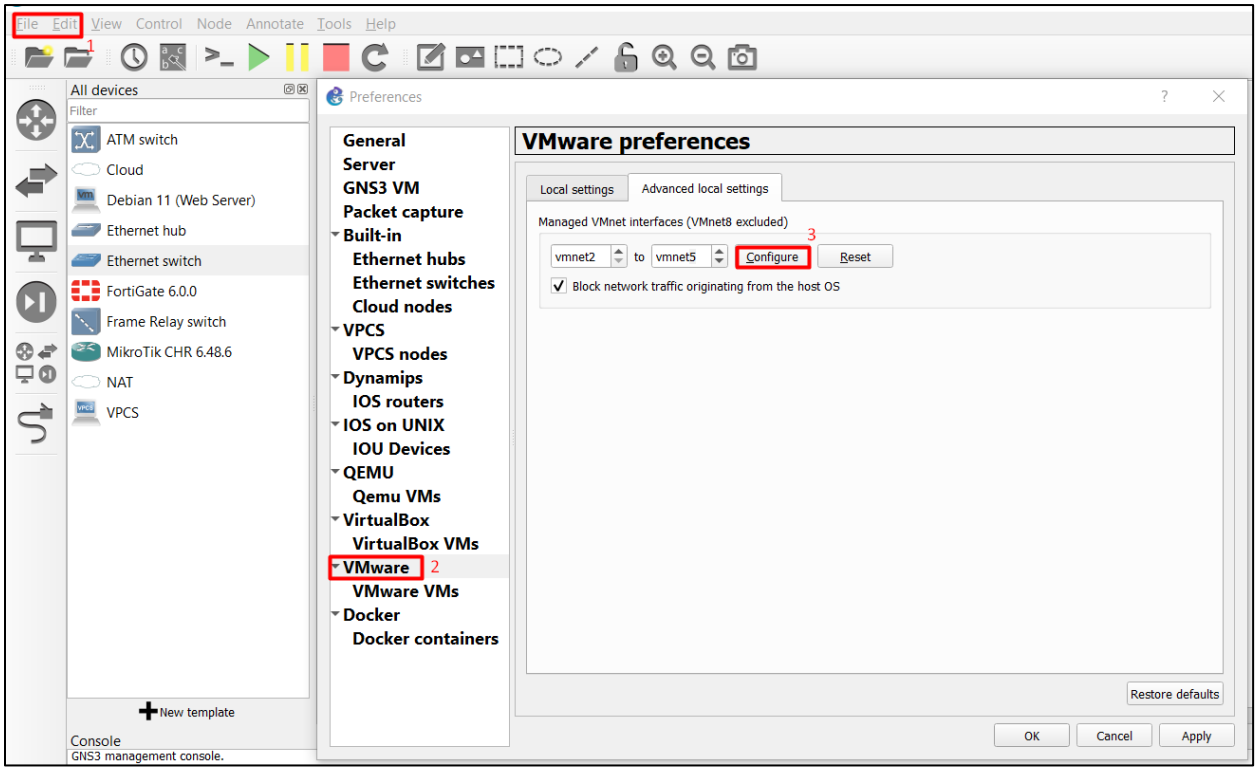


Figure 46 Error correction of GNS3 test case 1

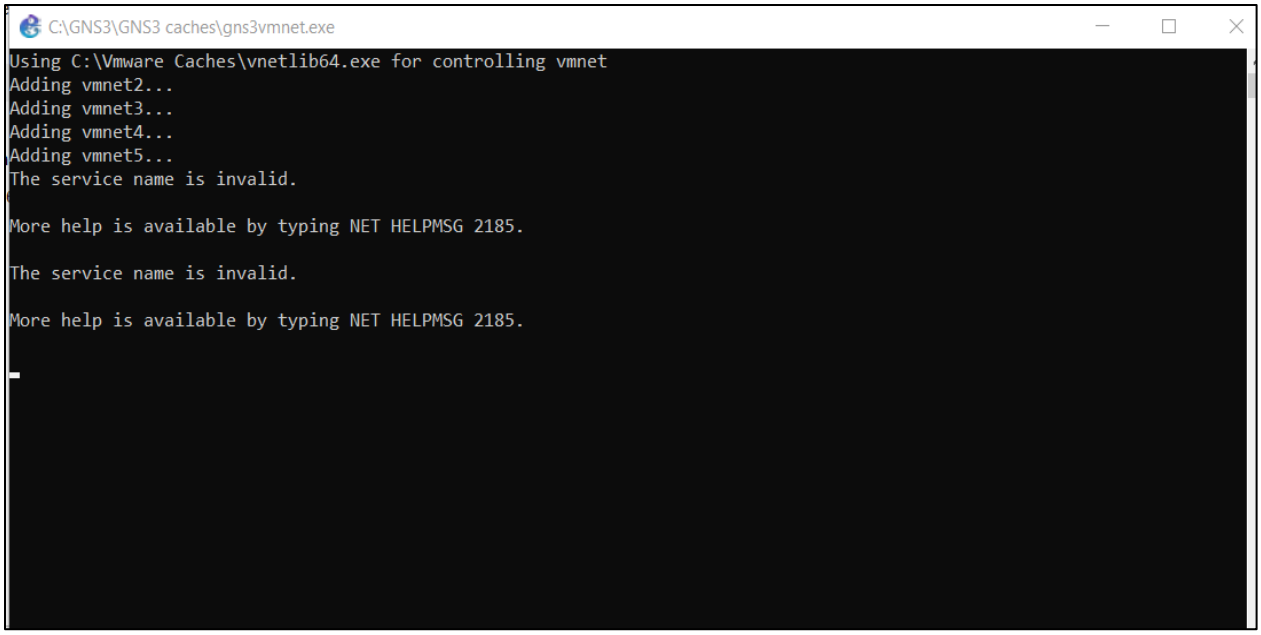


Figure 47 Error correction of GNS3 test case 1

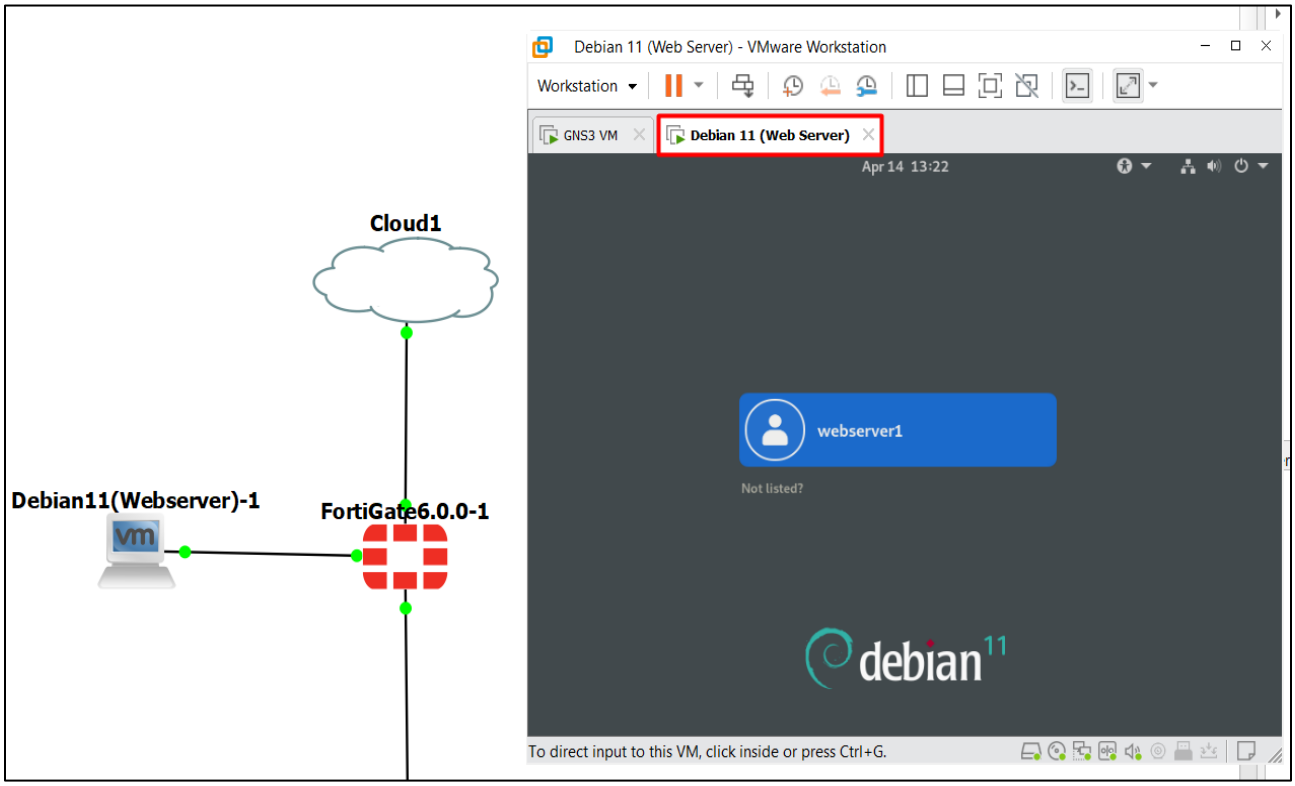


Figure 48 Test results: The VM node (Debian 11) operated automatically.

4.2.1.3. External web server test case

Test case 1	
Objective	To test whether the web server is installed in Debian 11 Linux or not.
Action	• Install web server by executing command “sudo apt-get install apache2” in CLI of Debian 11 Linux. • Check the status of webserver by executing command “systemctl status apache2.service”
Expected test Result	The active status should be “active (running)”
Actual test result	The active status is “active (running)”
Conclusion	Successfully done.

Table 16 External web server test case 1

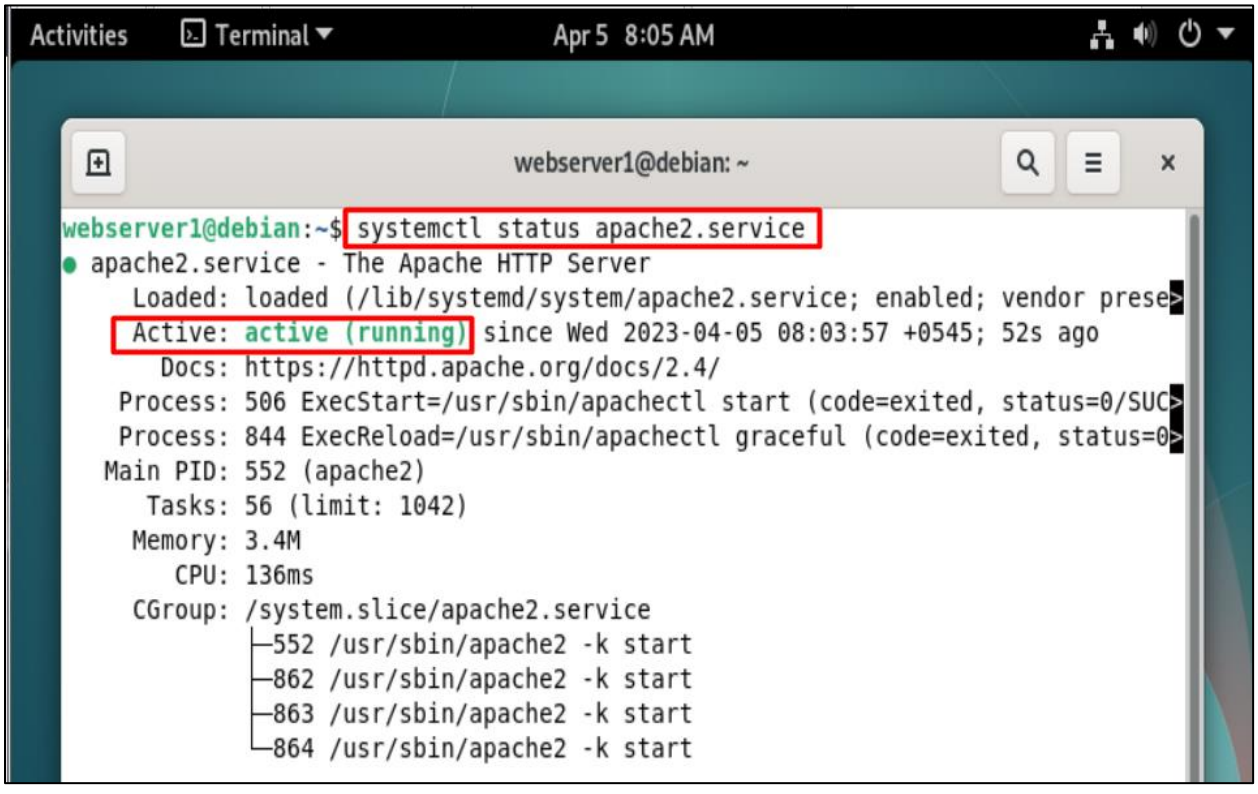


Figure 49 Test results: The web server is successfully installed in Debian 11 Linux.

4.2.1.4. FortiGate firewall test cases

Test case 1	
Objective	To test whether the FortiGate firewall is properly installed or not.
Action	• Add FortiGate firewall QEMU appliance in gns3 VM server. • Start the firewall and open console.
Expected test Result	The firewall console should not display any license error message.
Actual test result	The firewall console was displaying a license error message.
Error	The assigned RAM was 2 GB, but exceeding limit of RAM was 1 GB, thus causing licensing error.
Correction	1 GB RAM is allocated to firewall.
Conclusion	Successfully done. The console was not displaying any license error message.

Table 17 FortiGate firewall test case 1

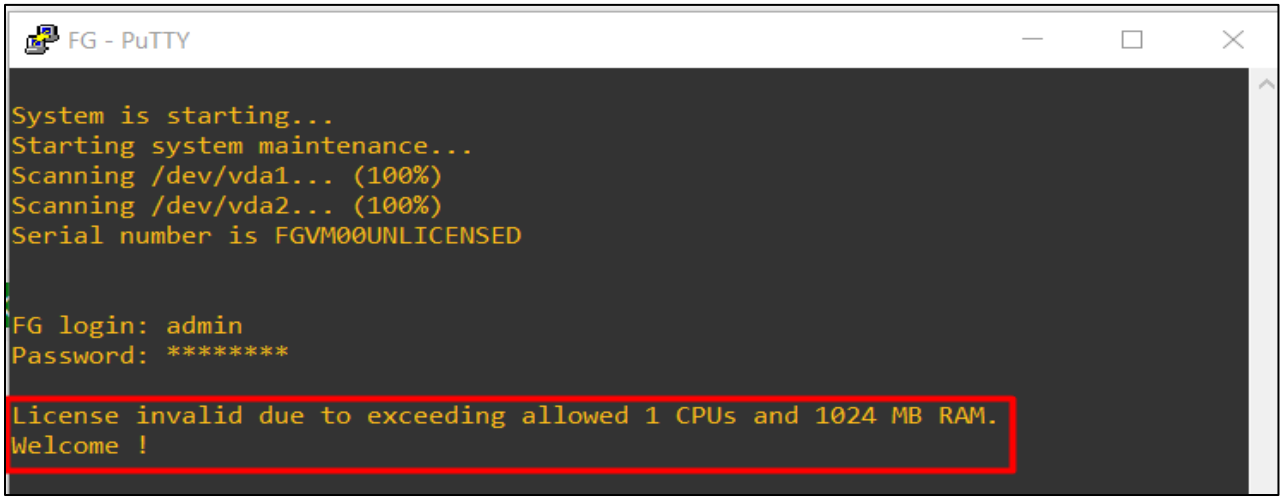


Figure 50 Error of FortiGate firewall test case 1

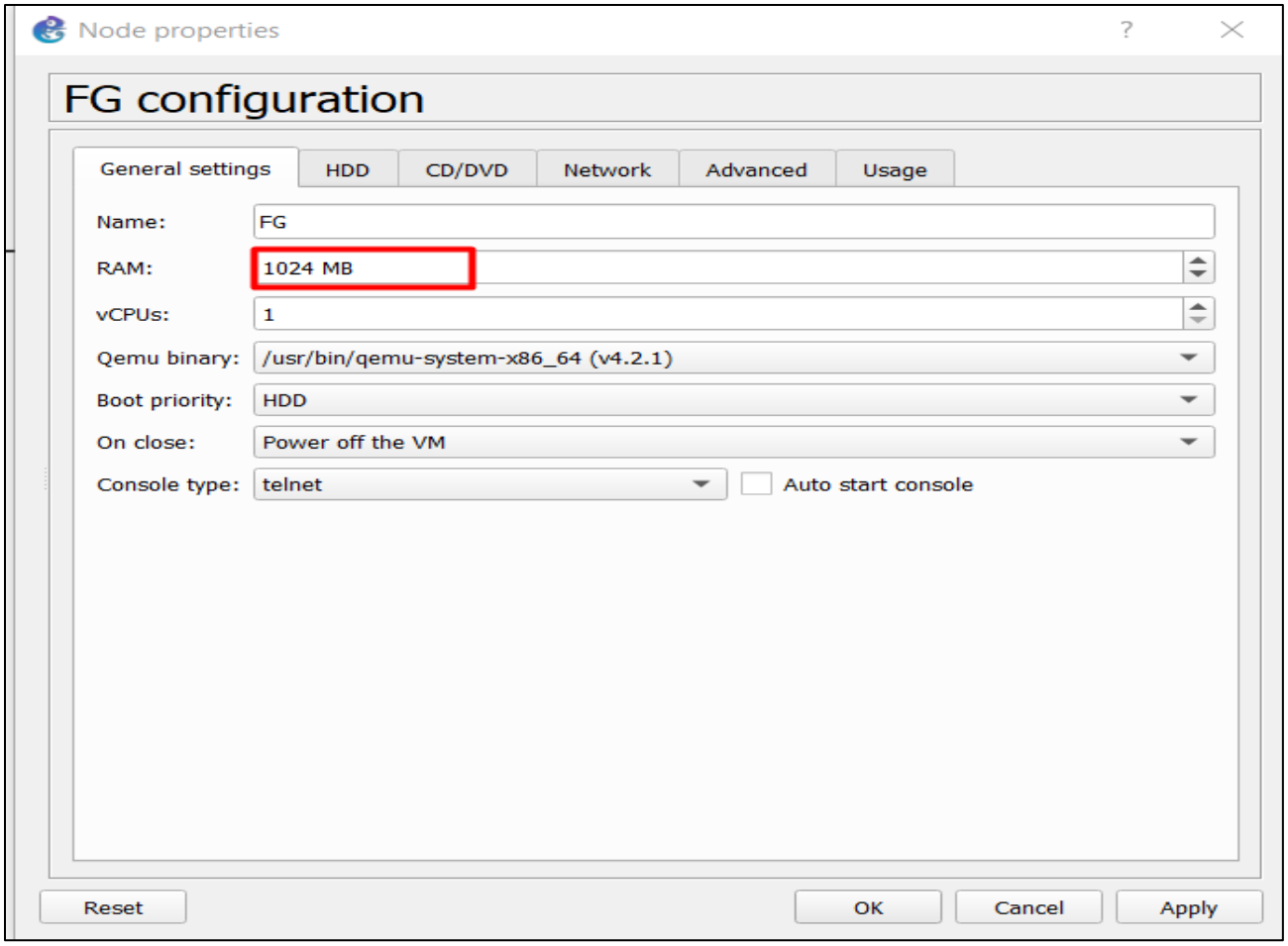


Figure 51 Error correction of FortiGate firewall test case 1.

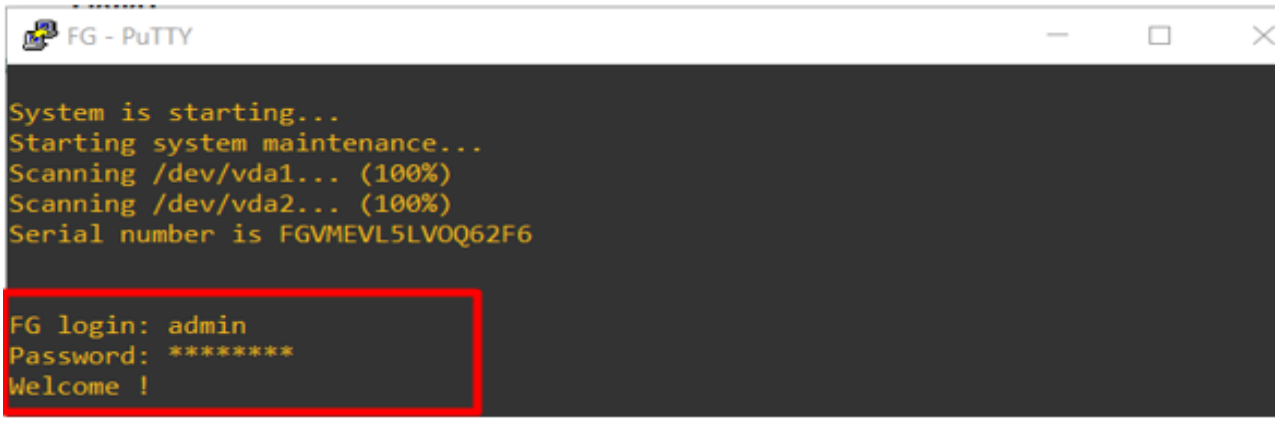


Figure 52 Test results: the licensing error was successfully eliminated.

Test case 2	
Objective	To test whether the FortiGate firewall GUI is accessible or not.
Action	• Assign IP address ranging within the ISP's network i.e. • Access the GUI using the IP in any browser.
Expected test Result	The firewall GUI should be accessible.
Actual test result	The firewall's GUI is not accessible.
Error	The route was not assigned properly.
Correction	New static route is configured, setting the default gateway of ISP cloud node.
Conclusion	Successfully done. The GUI was accessible now.

Table 18 FortiGate firewall test case 2

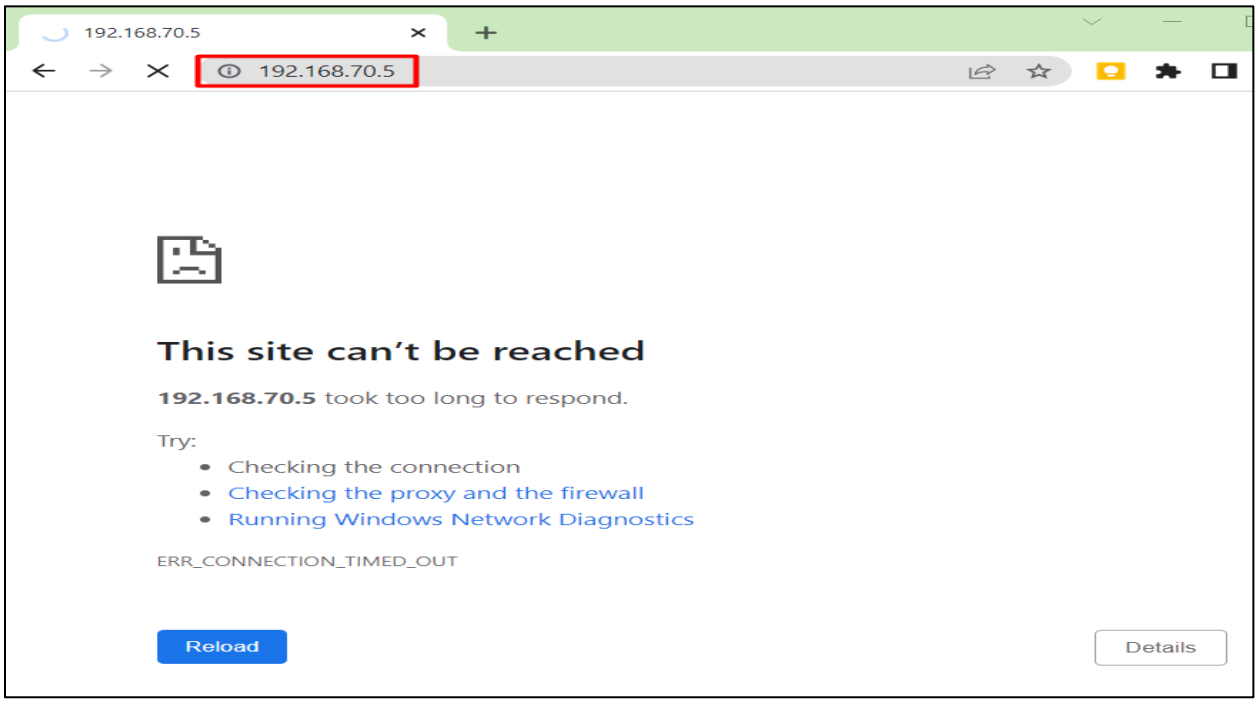


Figure 53 Error of FortiGate firewall test case 2.

```
FG # config router static

FG (static) # edit 1

FG (1) # set dst 0.0.0.0/0

FG (1) # set device port1

FG (1) # set gateway 192.168.70.2

FG (1) # end

FG # show system interface
config system interface
    edit "port1"
        set vdom "root"
        set ip 192.168.70.5 255.255.255.0
        set allowaccess ping https ssh http telnet
        set type physical
        set alias "WAN"
        set role wan
        set snmp-index 1
    next
```

Figure 54 Error correction of FortiGate firewall test case 2.

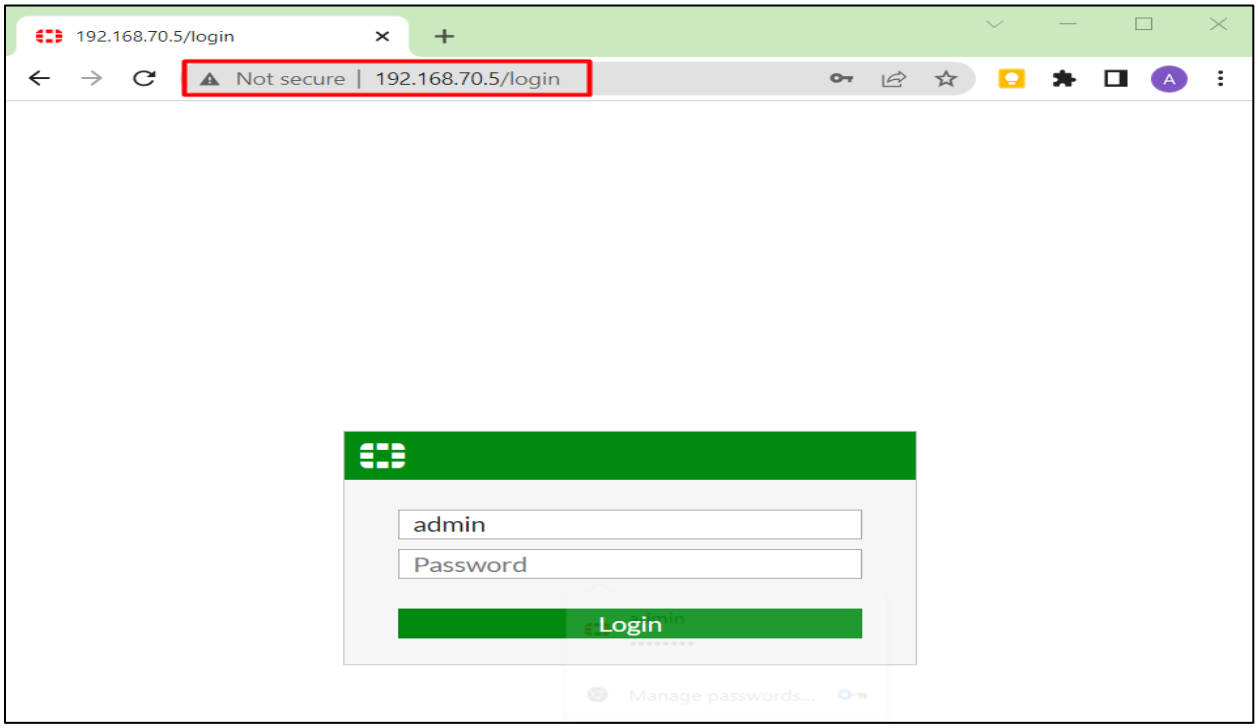


Figure 55 Test results: The GUI of the FortiGate firewall was accessible.

Test case 3	
Objective	To test the connectivity between the internal LAN and firewall.
Action	Start a VM node in internal LAN and ping the IP assigned to the firewall's LAN connecting interface.
Expected test Result	The ping should be successful.
Actual test result	The ping is not successful.
Error	DHCP server was not enabled.
Correction	Enable DHCP server on the interface that connects internal network with firewall.
Conclusion	Successfully done. The ping is successful.

Table 19 FortiGate firewall test case 3

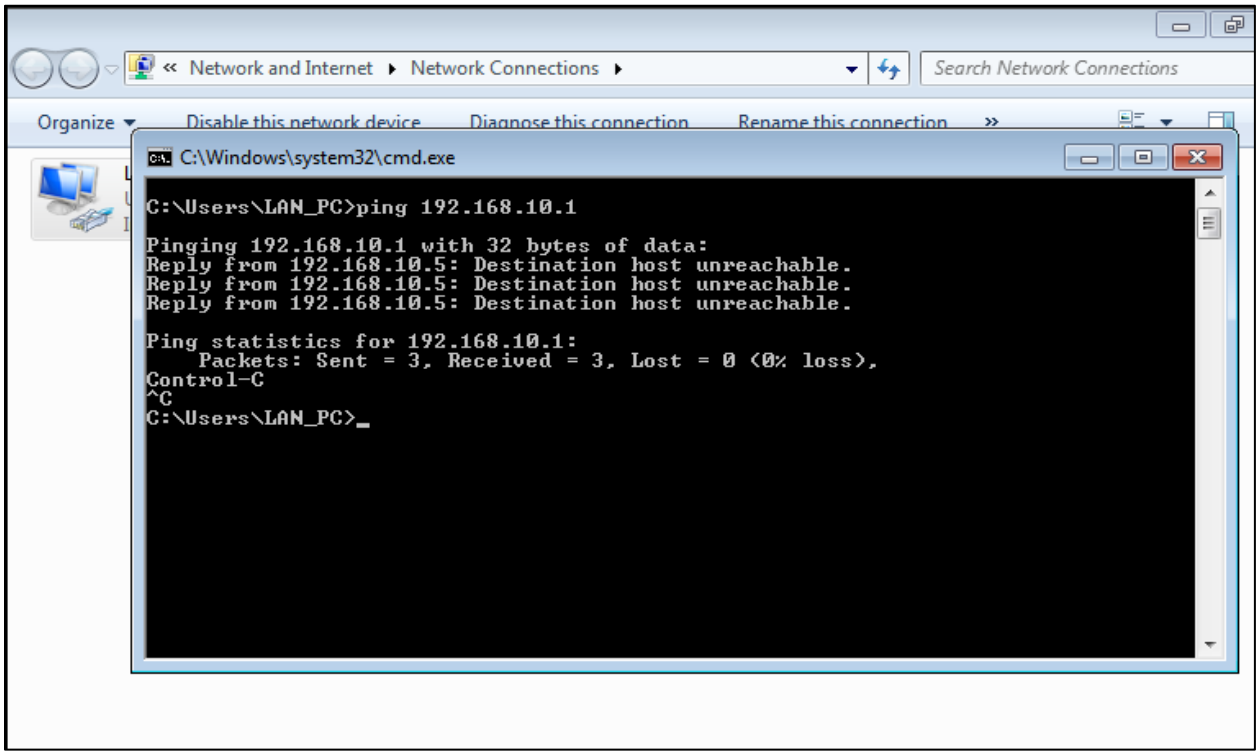


Figure 56 Error of FortiGate firewall test case 3

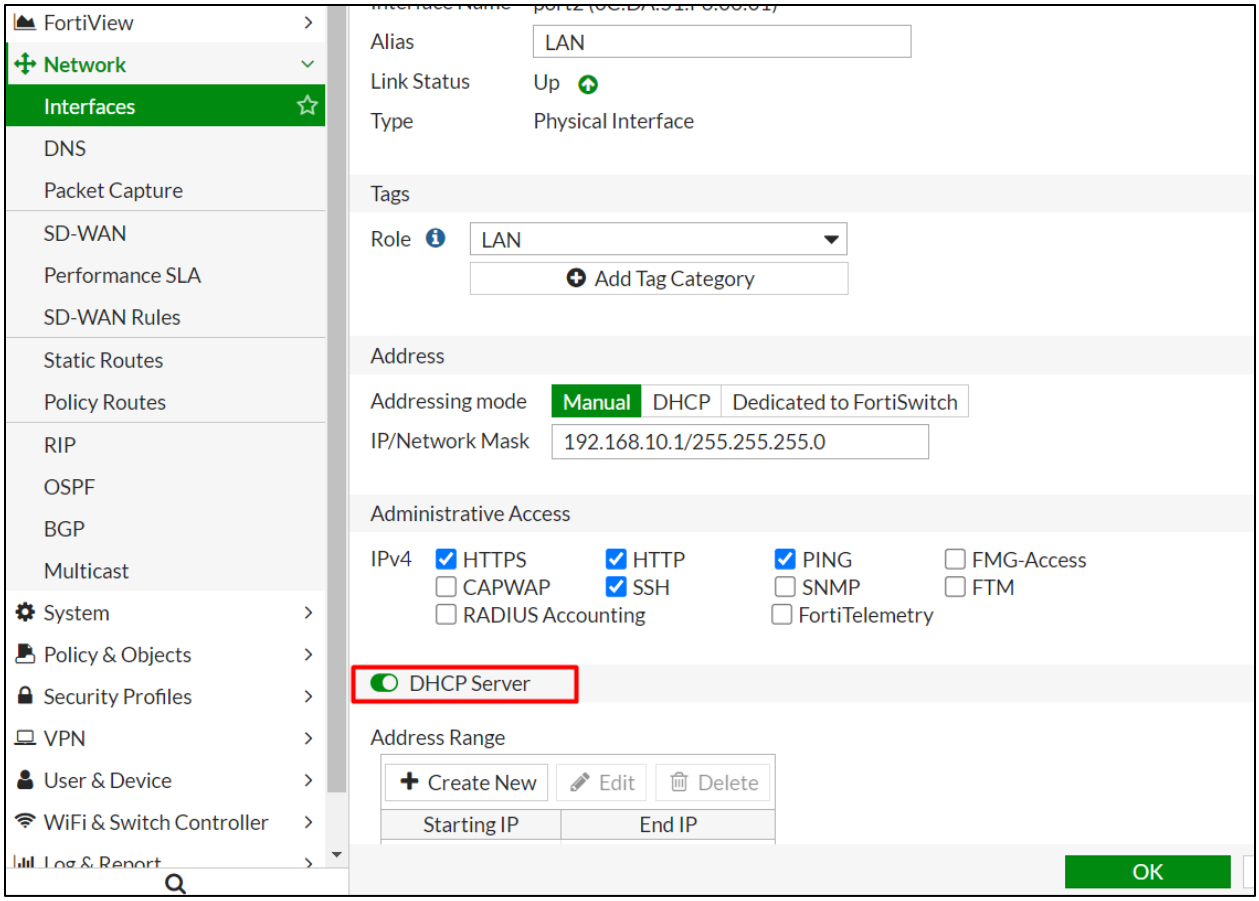


Figure 57 Error correction of FortiGate firewall test case 3

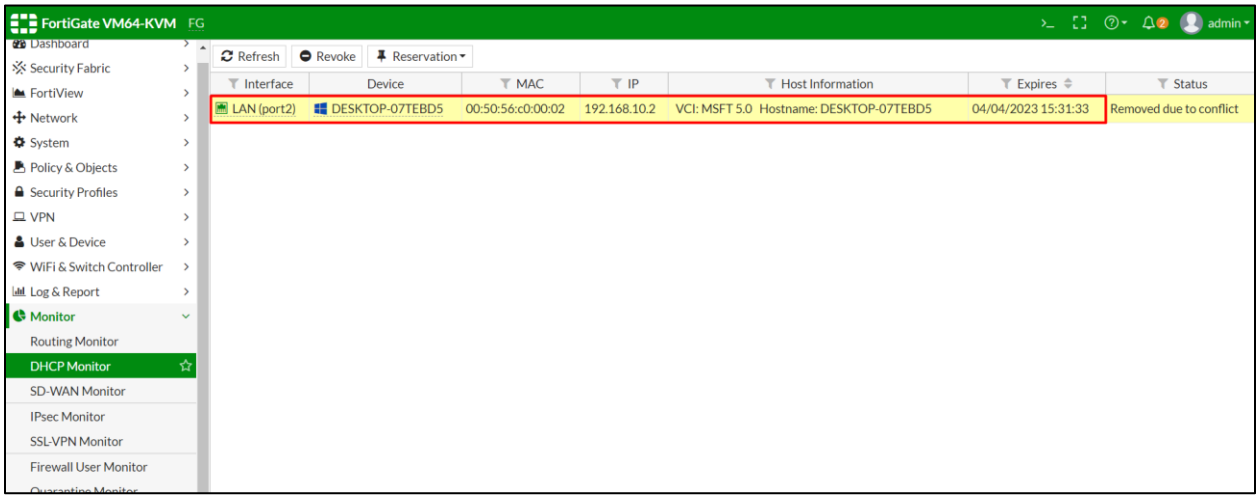


Figure 58 Error of FortiGate firewall test case 3

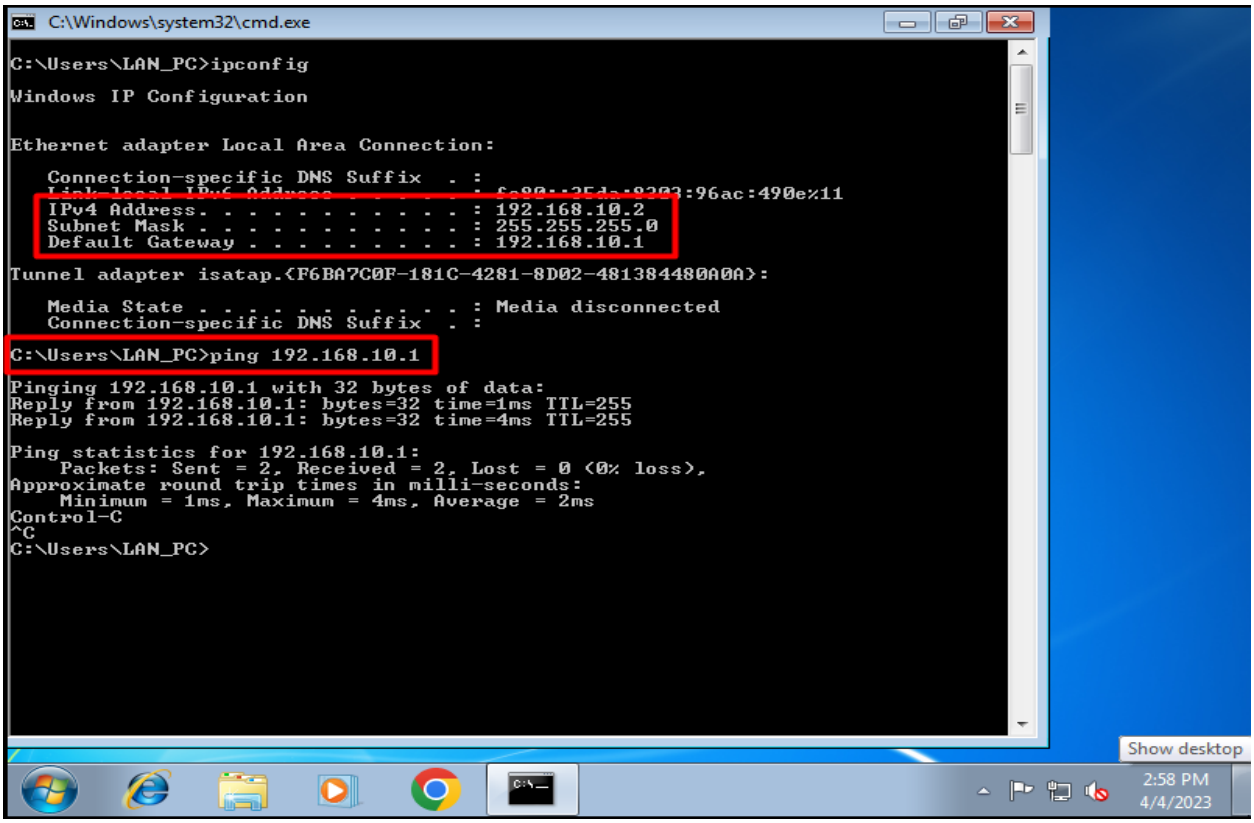


Figure 59 Test result: The DHCP is automatically assigned, and ping is successful.

Test case 4	
Objective	To test the status of internet connection in internal LAN.
Action	• Adda firewall policy to pass internet through LAN. • Start a PC in internal LAN and ping the google DNS i.e., 8.8.8.8
Expected test Result	The ping should be successful.
Actual test result	The ping is successful.
Error	Successfully done.

Table 20 FortiGate firewall test case 4

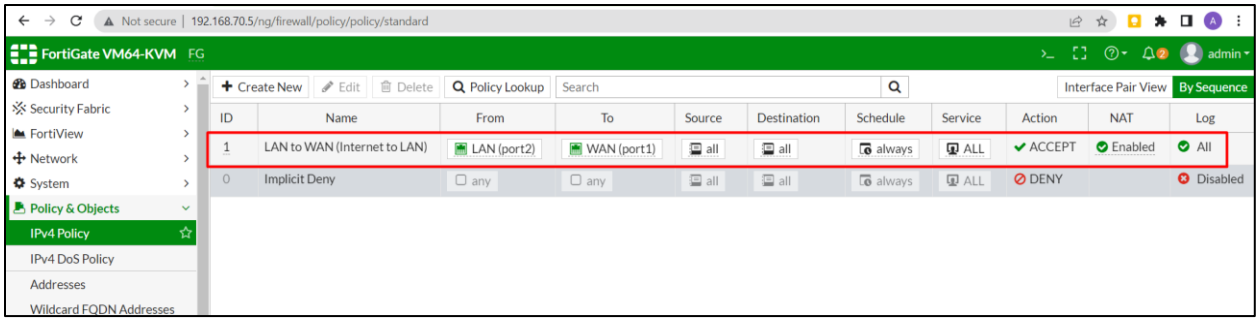


Figure 60 Firewall policy to allow internet in internal network.

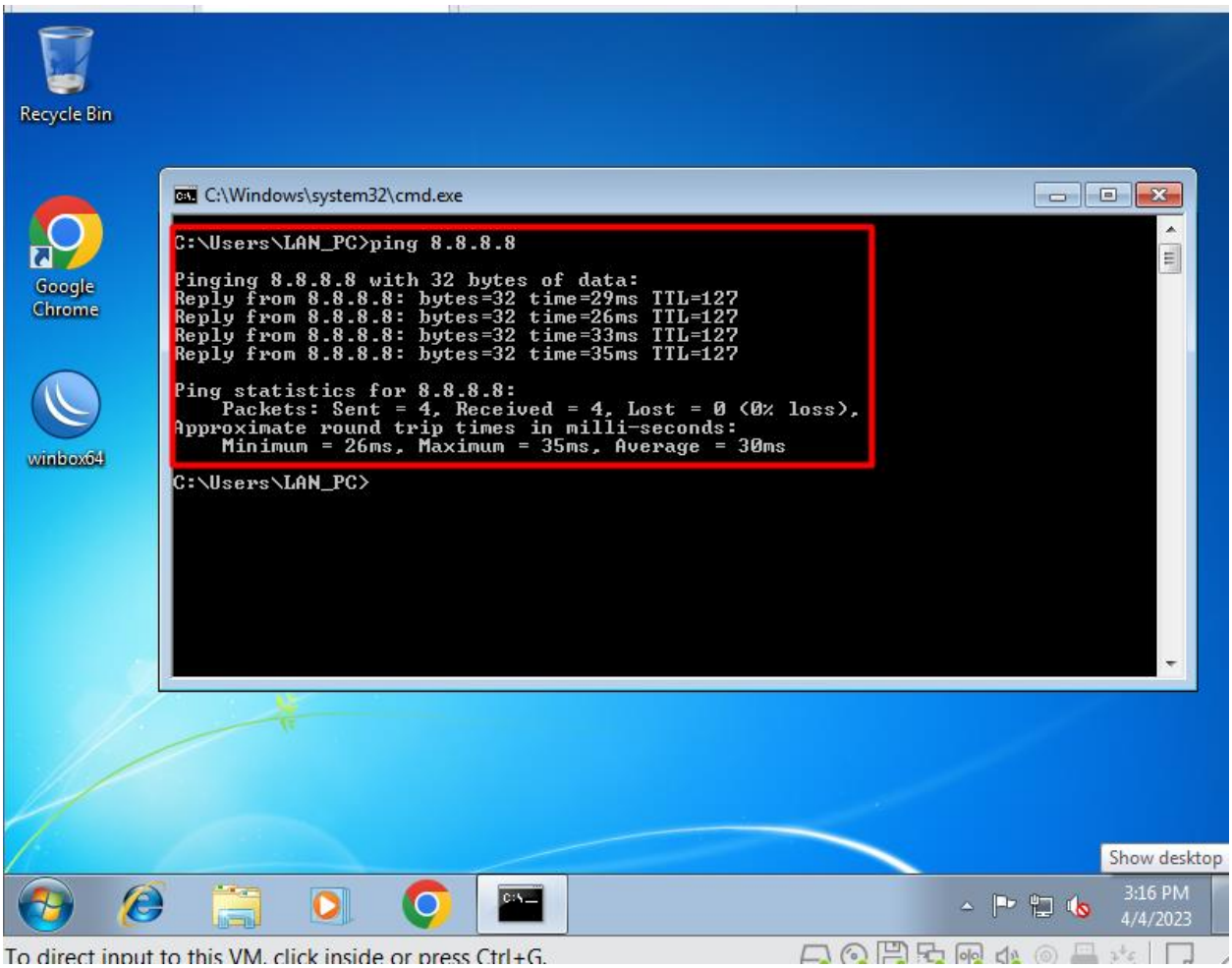


Figure 61 Test results: The PC from internal network is pinging the google DNS successfully.

Test case 5	
Objective	To test the connectivity between external web server and firewall for proper DMZ implementation.
Action	• Assign static IP in web server. • ping the gateway IP assigned to the DMZ interface of firewall.
Expected test Result	The ping should be successful.
Actual test result	The ping is successful.
Conclusion	Successfully done. The web server is now ready for DMZ implementation.

Table 21 FortiGate firewall test case 5

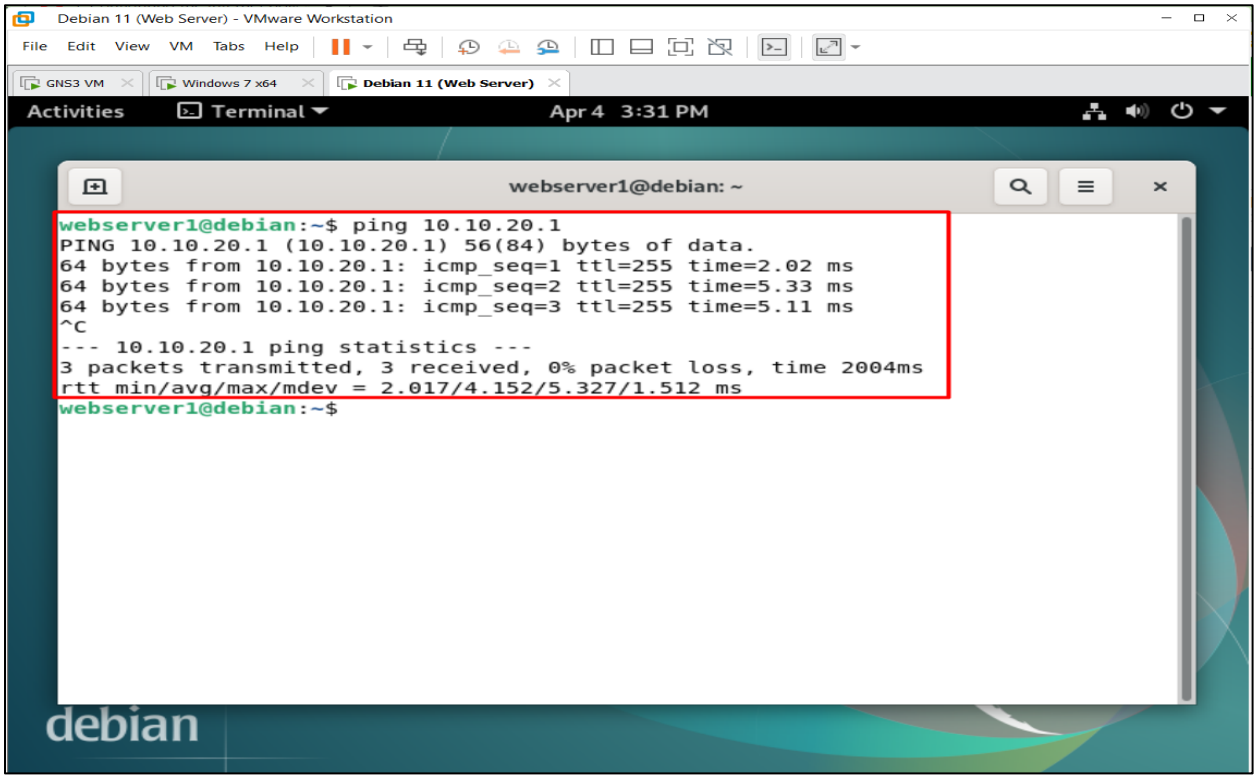


Figure 62 Test results: the external web server is configured successfully for DMZ implementation.

4.2.1.5. Miktrotik test cases

Test case 1	
Objective	To test whether there is any loss of internet connectivity on the interface connecting ESXi or not.
Action	• Use the speed test tool. • Provide the interface IP and start testing.
Expected test Result	There should be 0% connectivity loss.
Actual test result	There is 0% connectivity loss.
Conclusion	Successfully done. The internet connectivity was fine on ESXi interface.

Table 22 Miktrotik test case 1

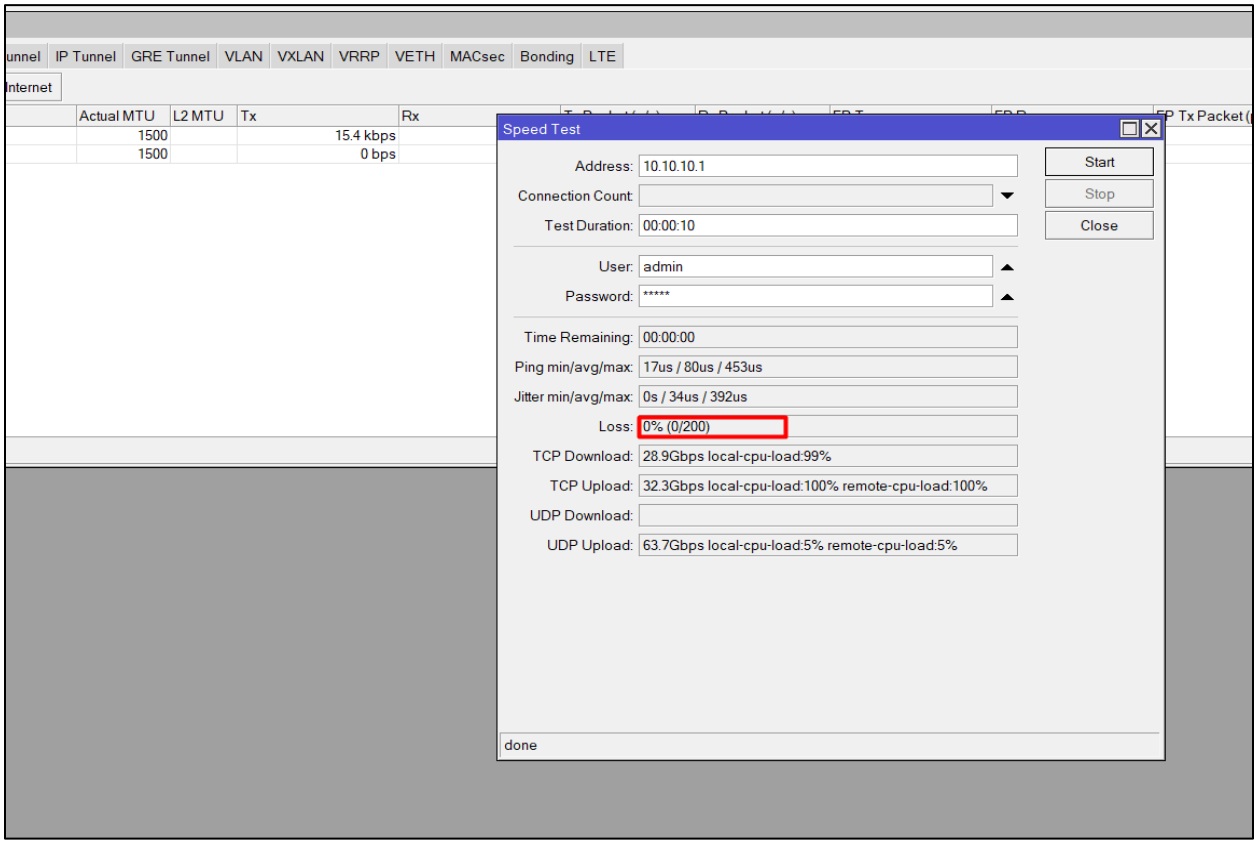


Figure 63Test results: 0% connectivity loss on the ESXi connecting interface.

Test case 2	
Objective	To test whether the router can communicate with all the VMs inside ESXi or not.
Action	Ping IP address of all the VMs (Domain controller, Web server, CL1 and CL2) configured on ESXi.
Expected test Result	The ping should be successful.
Actual test result	The ping is successful.
Conclusion	Successfully done.

Table 23 Miktrotik test case 2

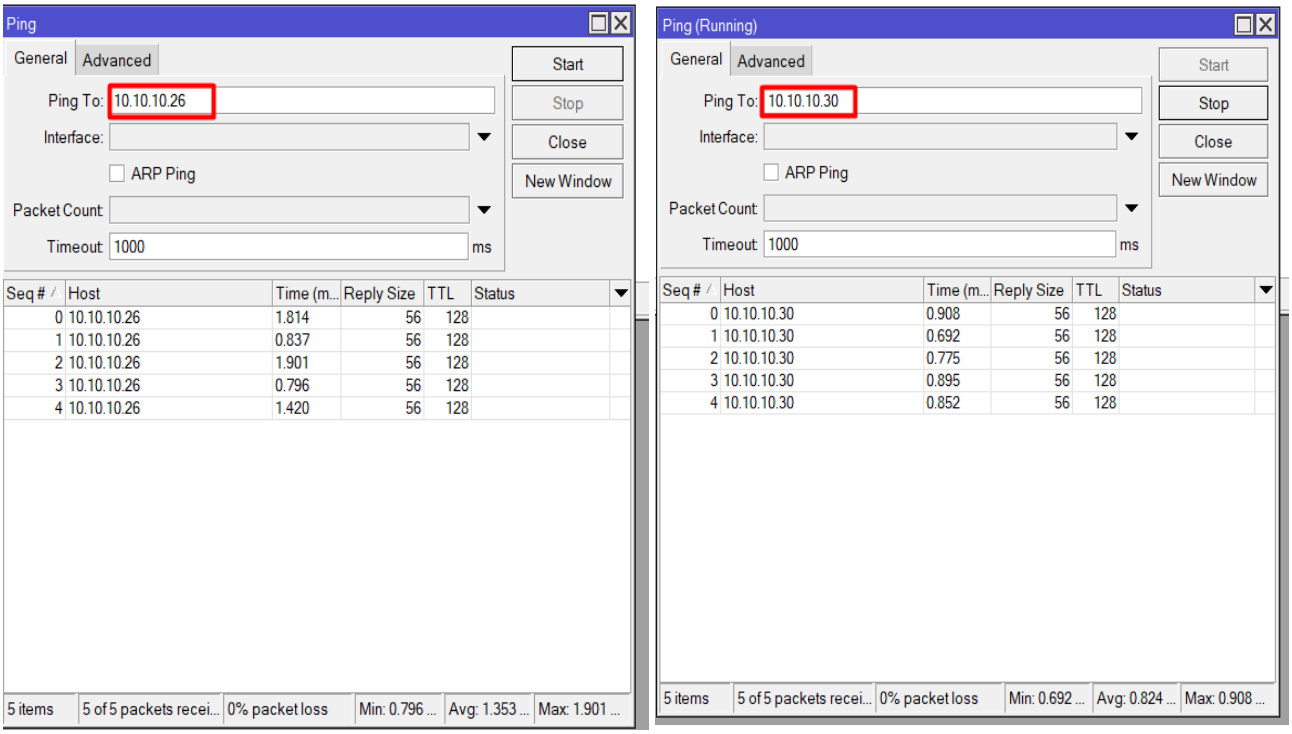


Figure 64 Test result: the router is successfully communicating with the DC and internal web server in ESXi,

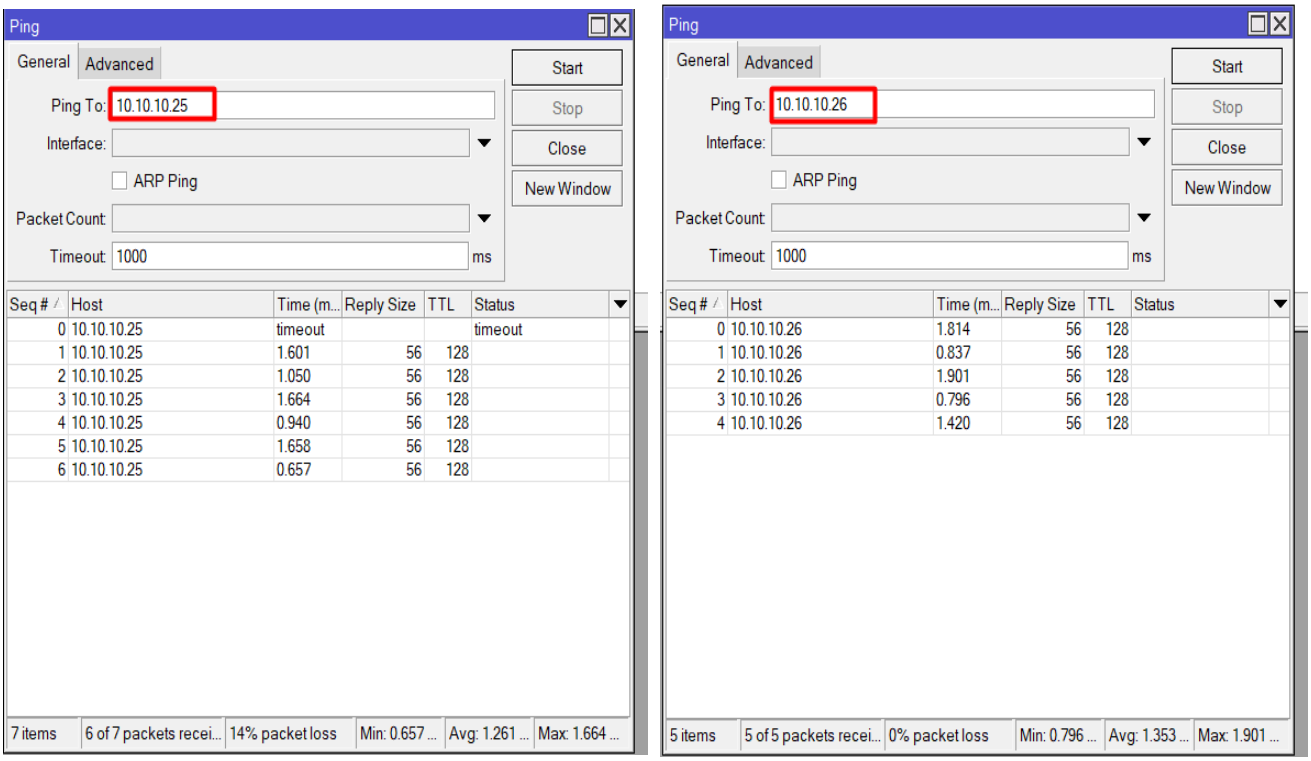


Figure 65 Test result: the router is successfully communicating with CL1 and CL2 in ESXi.

4.2.1.6. VMware ESXi test case

Test case 1	
Objective	To test whether the VMware ESXi is properly installed or not.
Action	• Install VMware ESXi 7 and connect to router. • Assign static IP address. • Access GUI of the ESXi.
Expected test Result	The GUI of VMware ESXi 7 should be accessible.
Actual test result	The GUI of VMware ESXi 7 is accessible.
Conclusion	Successfully done.

Table 24 VMware ESXi test case 1

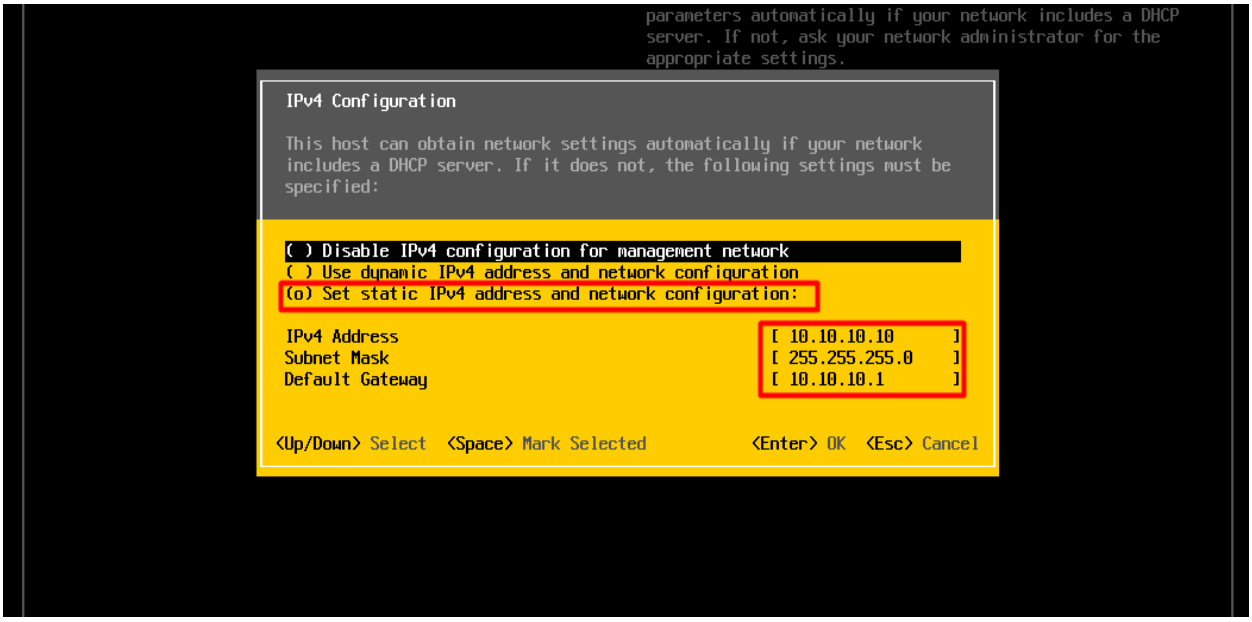


Figure 66 Assigning static IP address in ESXi.

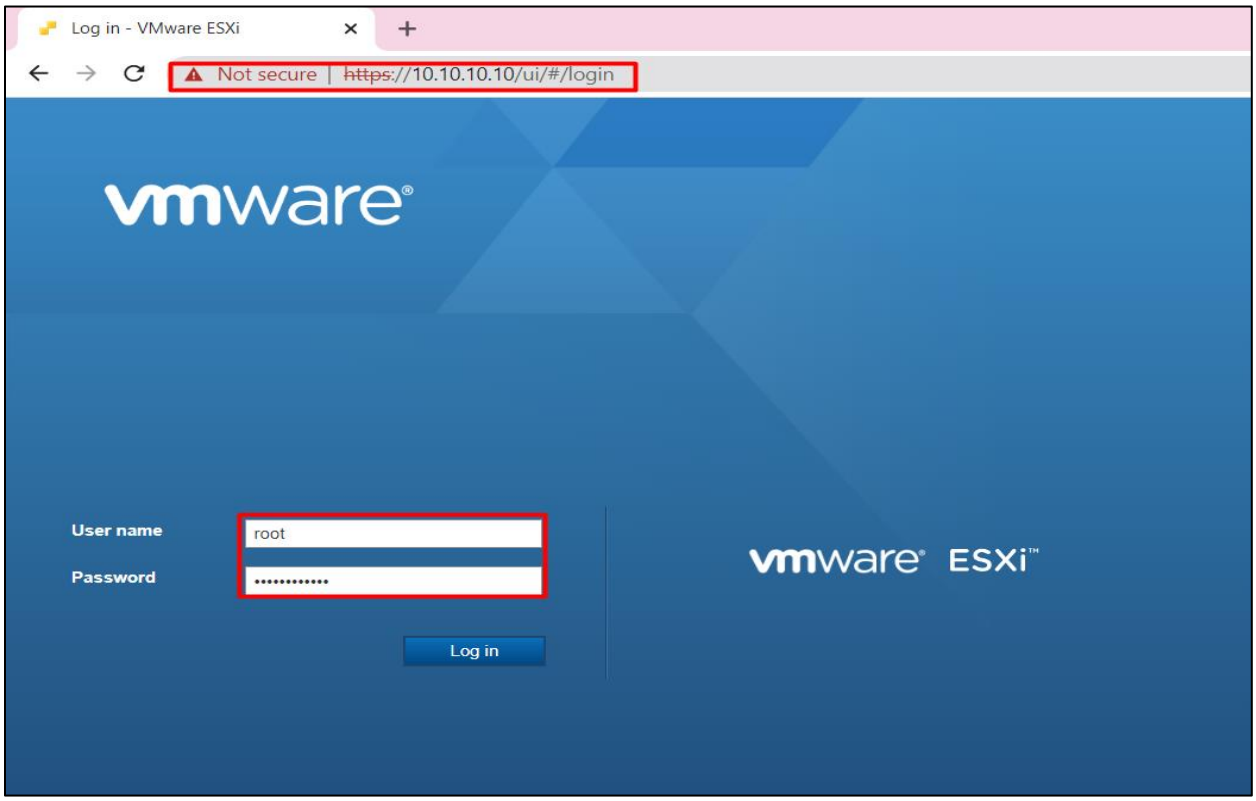


Figure 67 Test results: The GUI of VMware ESXi is accessible.

Test case 2	
Objective	To test whether the increment of the datastore is successful or not.
Action	• Select expand the capacity of datastore in GUI. • Expand the capacity as per needed.
Expected test Result	The datastore's capacity should increase.
Actual test result	The datastore's capacity was not increased.
Error	An error message "Failed to increase VMFS datastore datastore1" was shown.
Correction	The following commands were used in SSH console. "partedUtil getptbl '/vmfs/devices/disks/mpx.vmhba0: C0:T0: L0'" "partedUtil resize '/vmfs/devices/disks/mpx.vmhba0: C0:T0: L0' 8 268437504 566231006
Conclusion	Successfully done. The capacity of the datastore was increased successfully.

Table 25 VMware ESXi test case 2

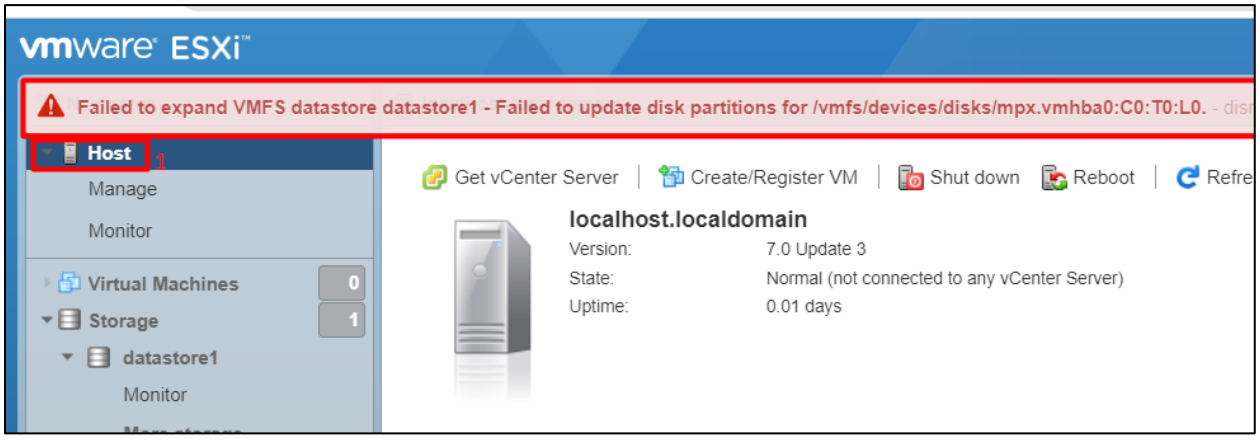


Figure 68 Error of VMware ESXi test case 2

Figure 69 Error correction of VMware ESXi test case 2

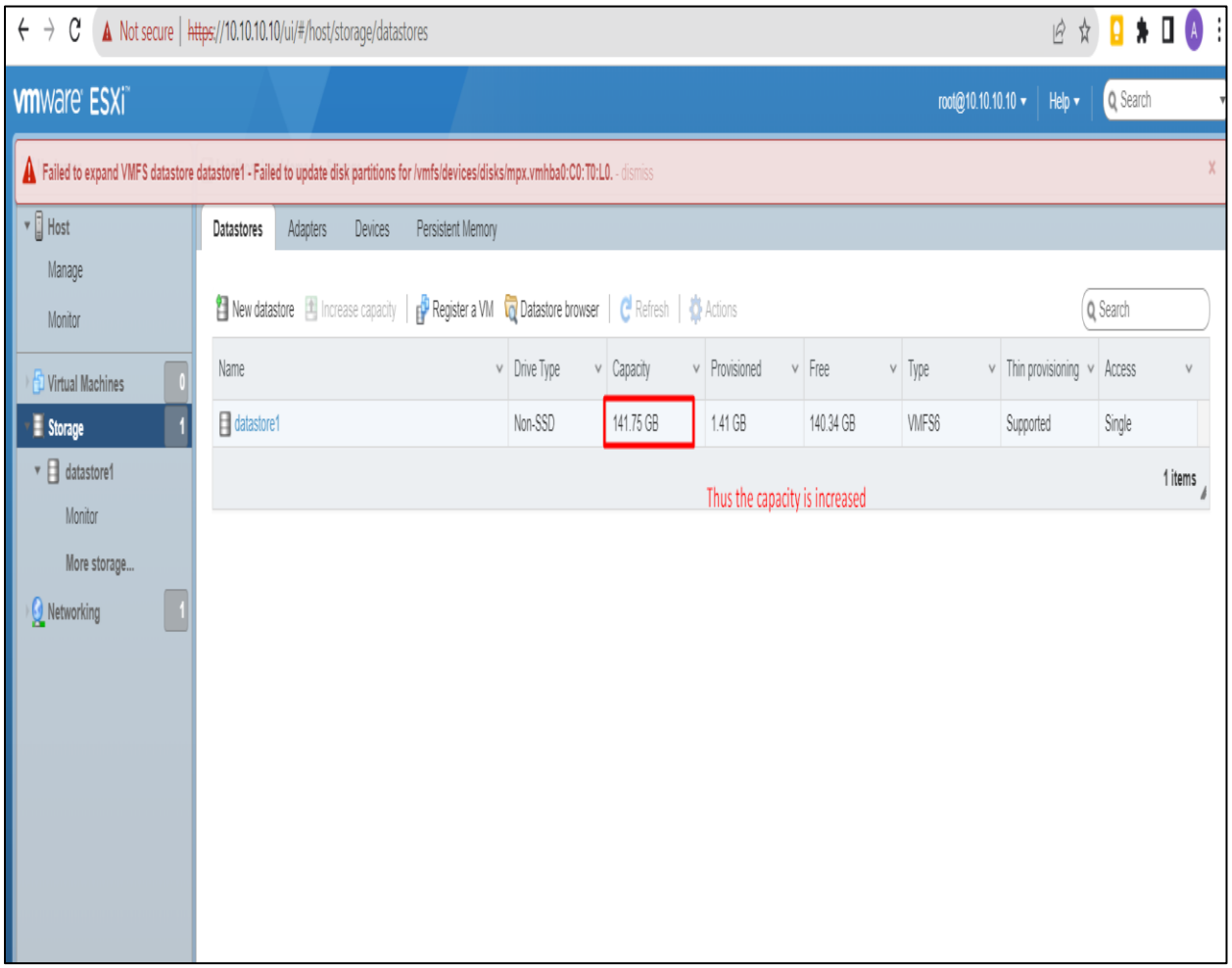


Figure 70 Tests results: The capacity of the datastore is increased successfully.

4.2.1.7. Domain controller test cases

Test case 1	
Objective	To test whether the DNS server is successfully installed and configured or not.
Action	"nslookup" command was entered in CLI.
Expected test Result	The server's name: EBL.com and Address: 10.10.10.20 should be displayed.
Actual test result	The server's name: EBL.com and Address: 10.10.10.20 is displayed.
Conclusion	Successfully done.

Table 26 Domain controller test case 1

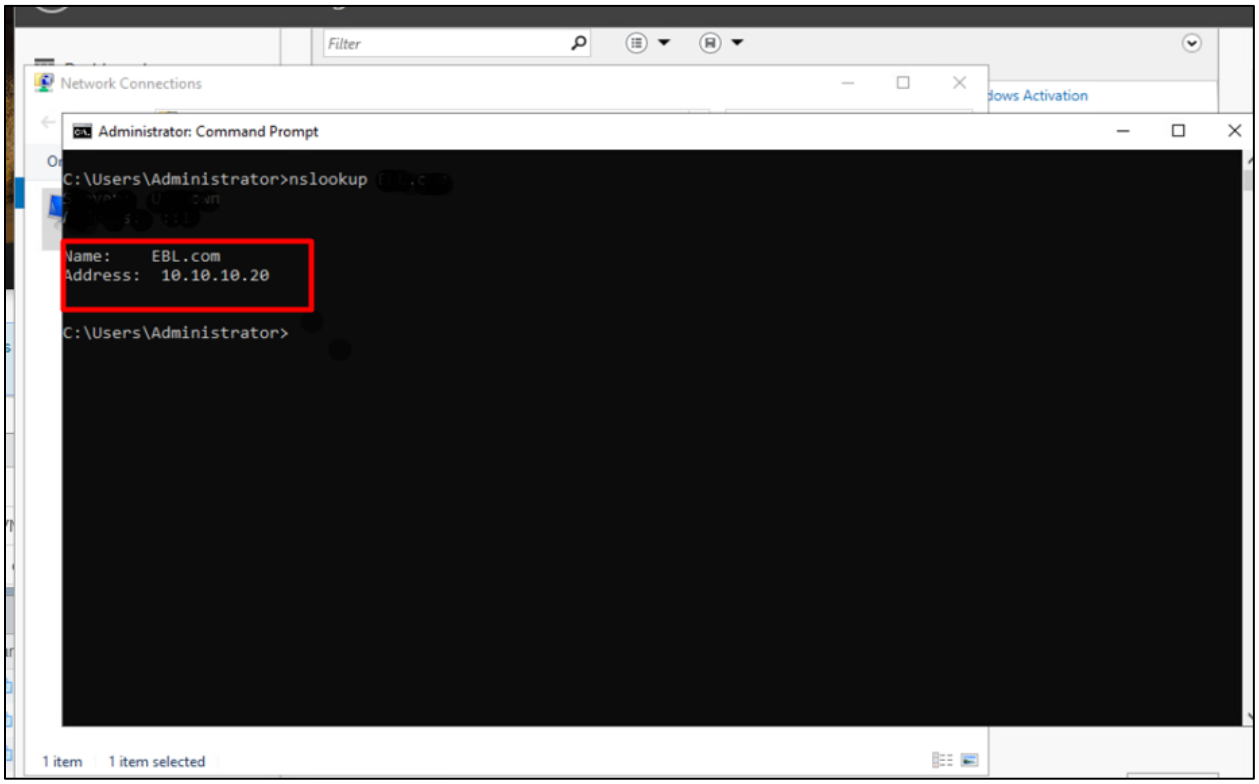


Figure 71 Test results: The DNS server is successfully installed.

Test case 2	
Objective	To test whether the computers are added in the domain controller or not.
Action	• Add the web server and two Client computers to EBL.com domain. • Check the list of added computers in AD computers list.
Expected test Result	The newly added computers should be displayed in AD (Active Directory) computers list.
Actual test result	The newly added computers are displayed in AD (Active Directory) computers list.
Conclusion	Successfully done.

Table 27 Domain controller test case 2

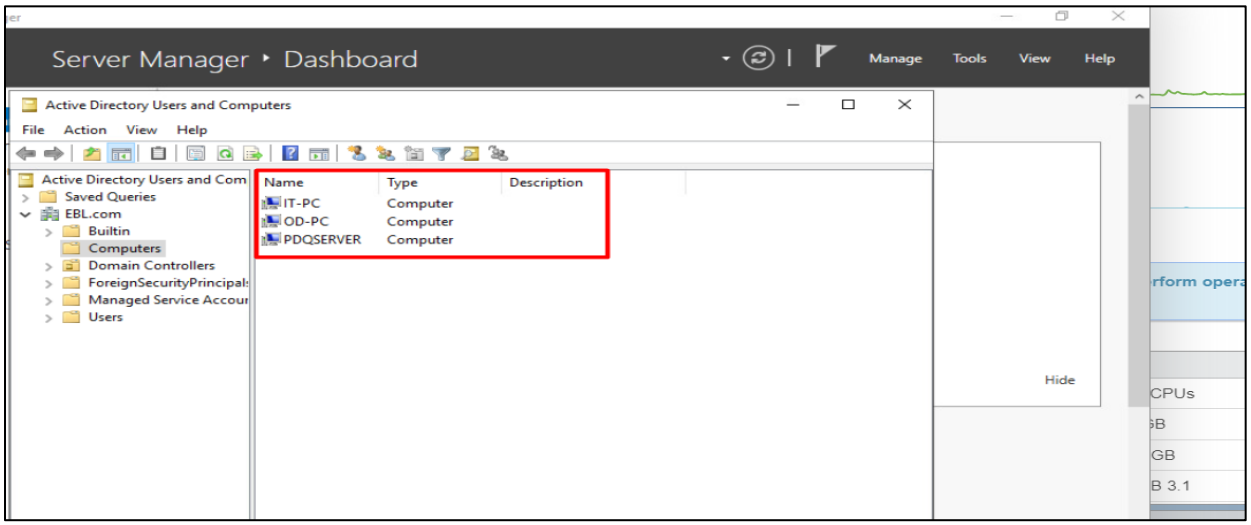


Figure 72 Test results: The computers are added successfully in DC.

4.2.1.8. Internal web server test cases

4.2.1.8.1. Lansweeper test case

Test case 1	
Objective	To test whether the LAN sweeper is installed properly or not.
Action	• Create a trial ID and register. • Install and run lansweeper.exe.
Expected test Result	The Lansweeper's GUI should be automatically opened in default web browser.
Actual test result	The Lansweeper's GUI is not started automatically in default web browser.
Error	The installation process was automatically aborted.
Correction	Installation of windows 2022 server because the windows 2019 server does not have .NET Framework 4.8 but for installing Lansweeper the server must have .NET Framework 4.8.
Conclusion	Successfully done. The Lansweeper's GUI started automatically.

Table 28 Internal web server (Lan sweeper) test case 1.

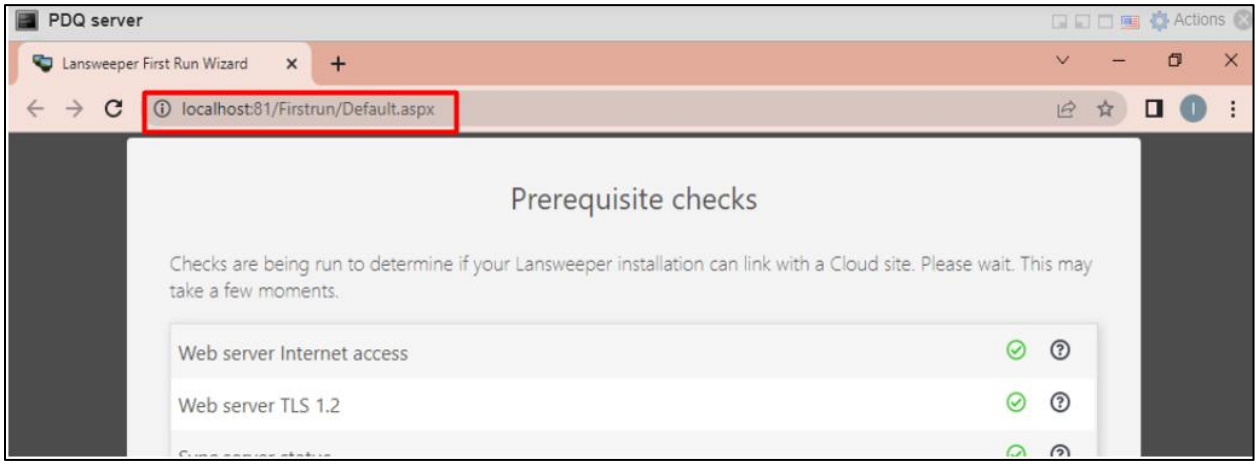


Figure 73 Test results: The LAN sweeper was installed successfully on windows server 2022.

Test case 2	
Objective	To test whether Lansweeper meet the perquisites to begin scanning.
Action	• Check the prerequisites availability.
Expected test Result	All the prerequisites should be fulfilled.
Actual test result	All the prerequisites are fulfilled.
Conclusion	Successfully done.

Table 29 Internal web server (Lan sweeper) test case 2.

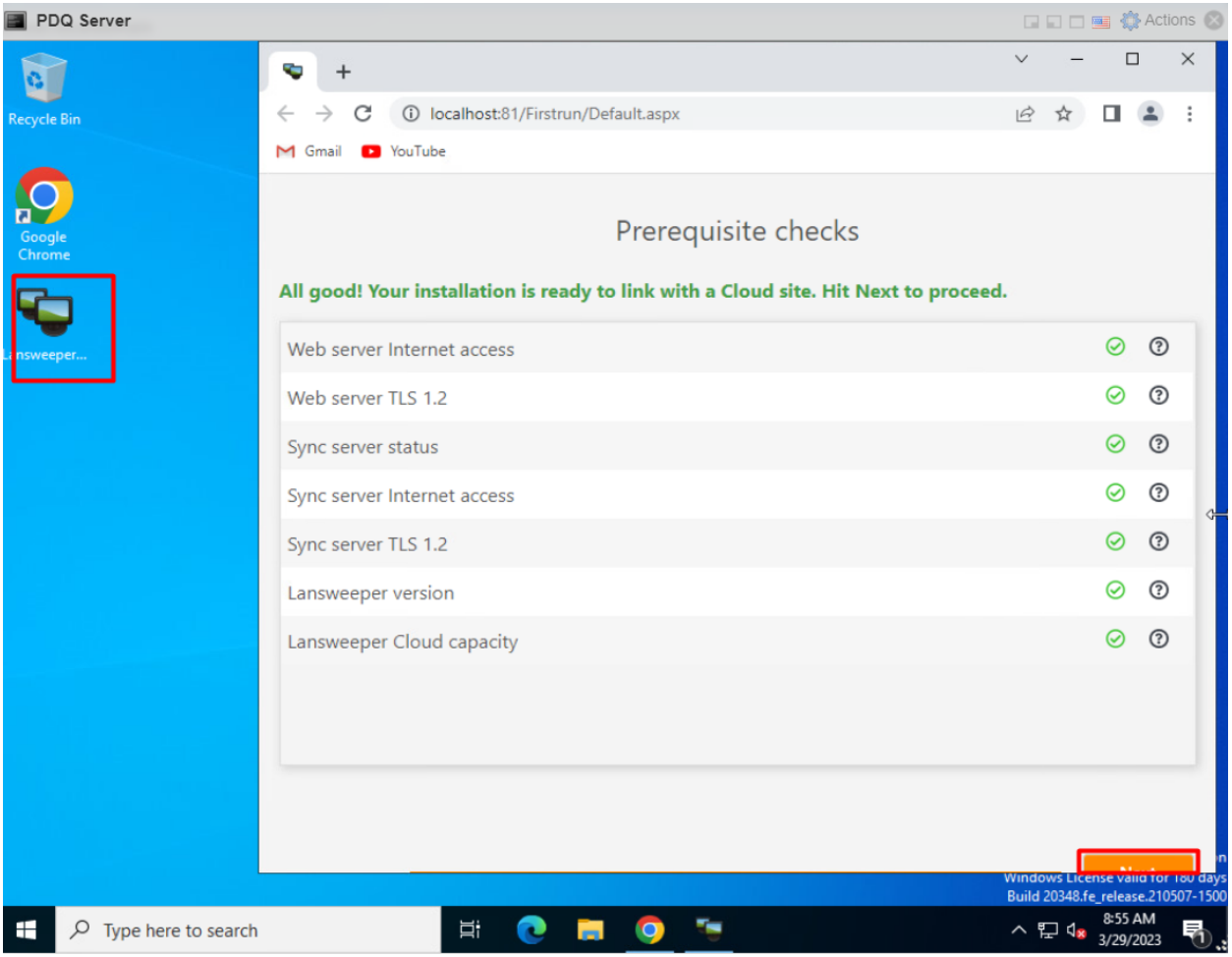


Figure 74 Test results: All prerequisites for the installation process of Lan sweeper are fulfilled.

4.2.1.8.2. PDQ deploy test cases

Test case 3	
Objective	To test whether the pdq deploy is installed in enterprise mode or not.
Action	• Download the installer image from official site. • Get the trial license key for enterprise mode. • Add the existing domain name.
Expected test Result	The PDQ deploy should operate successfully for EBL.com.
Actual test result	The PDQ deploy operated successfully for domainEBL.com.
Conclusion	Successfully done.

Table 30 Internal web server (PDQ deploy) test case 3.

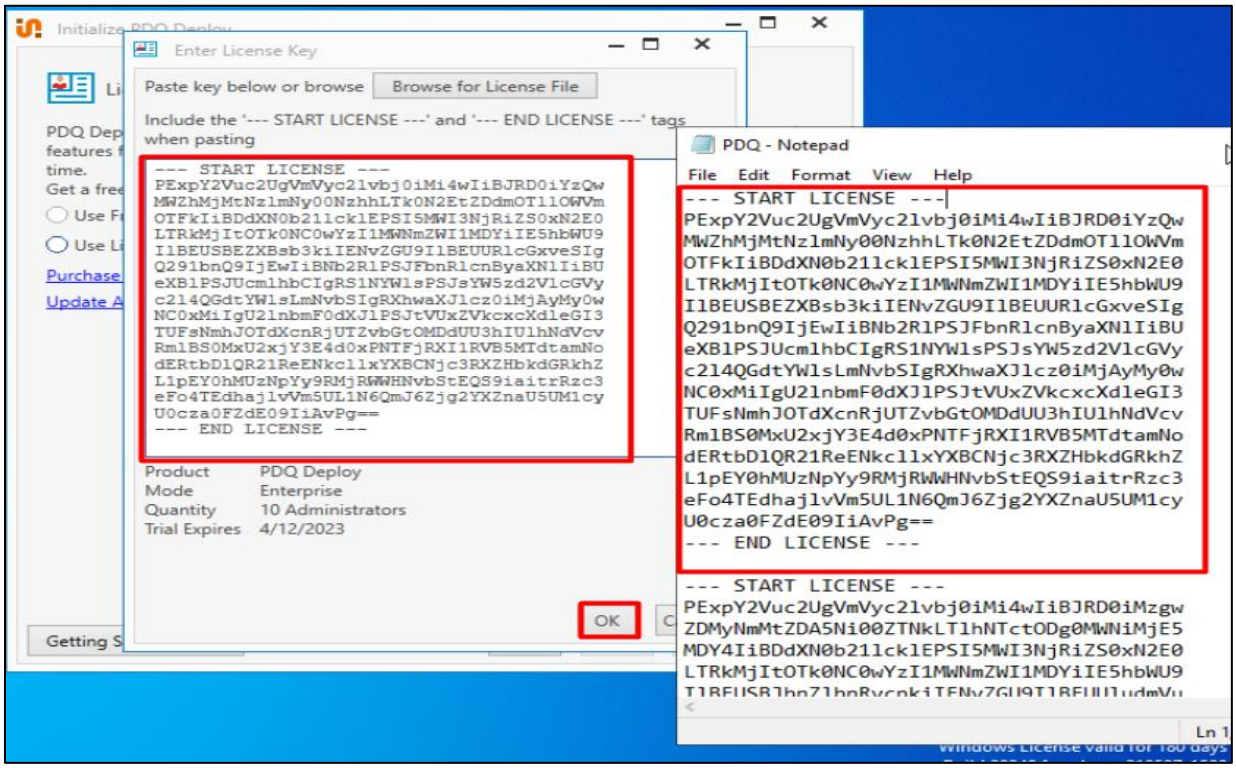


Figure 75 Applying trial enterprise license.

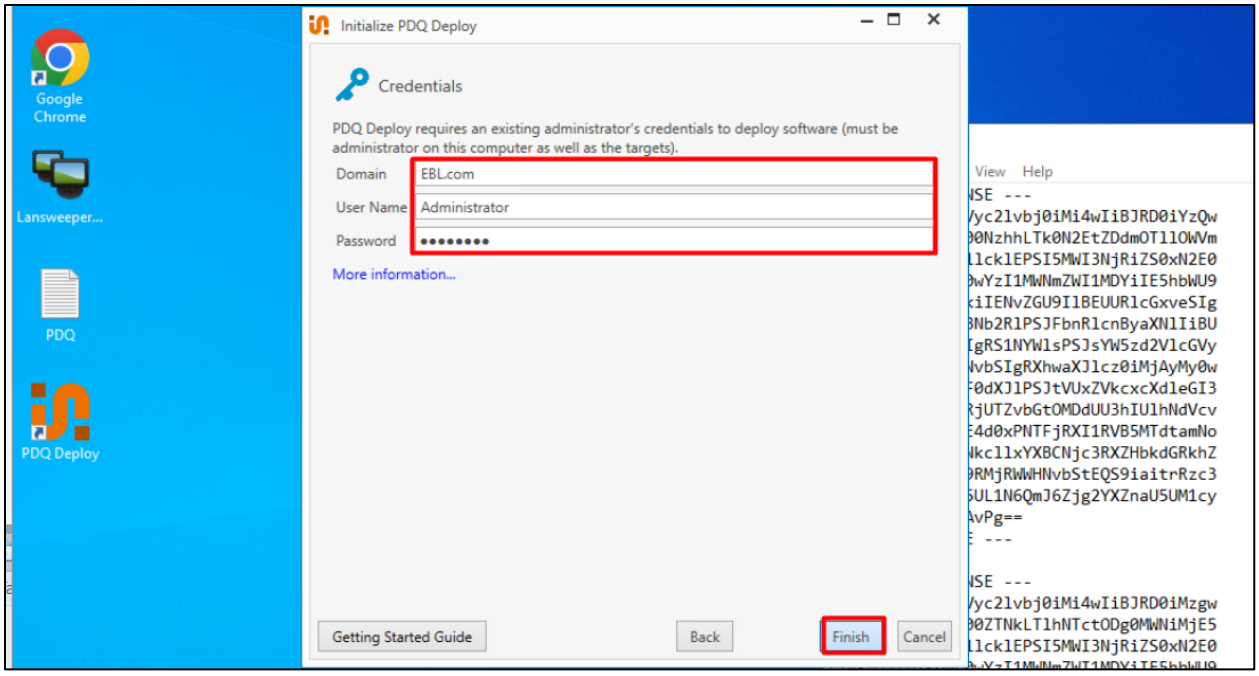


Figure 76 Adding domain in PDQ deploy.

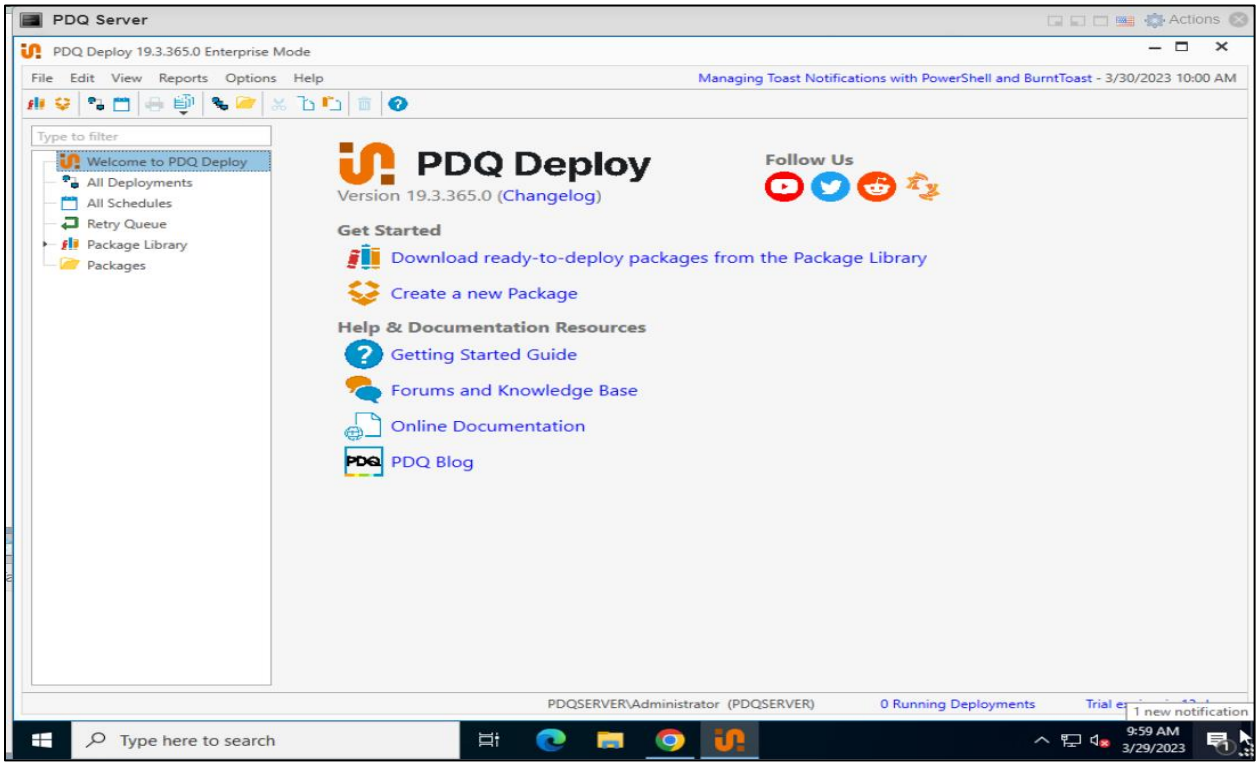


Figure 77 Test result: The PDQ deploy was installed in enterprise mode successfully.

4.2.2. System testing

4.2.2.1. Demilitarized zone test cases.

Test case 1	
Objective	To test whether the web server in DMZ is accessible by the internal users or not.
Action	• create virtual IPs for http and https connection. • Add firewall policy to access web server in DMZ.
Expected test Result	The default Apache webpage should be displayed after browsing webserver IP address (10.10.20.10).
Actual test result	The default webpage is displayed after browsing webserver IP address (10.10.20.10).
Conclusion	Successfully done. The internal users can access web server in DMZ.

Table 31 DMZ test case 1

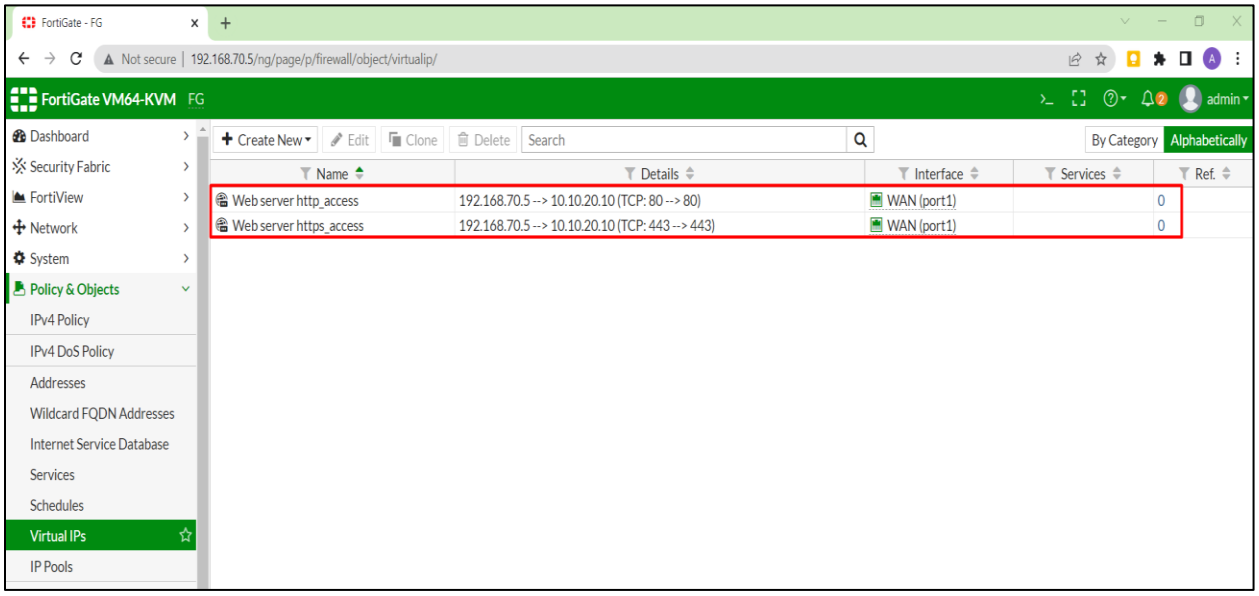


Figure 78 creating virtual IP for DMZ implementation.

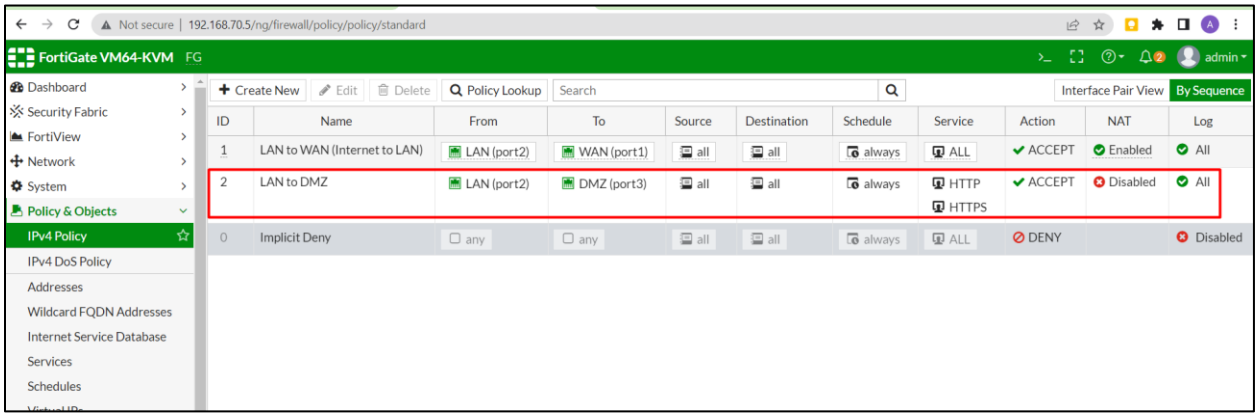
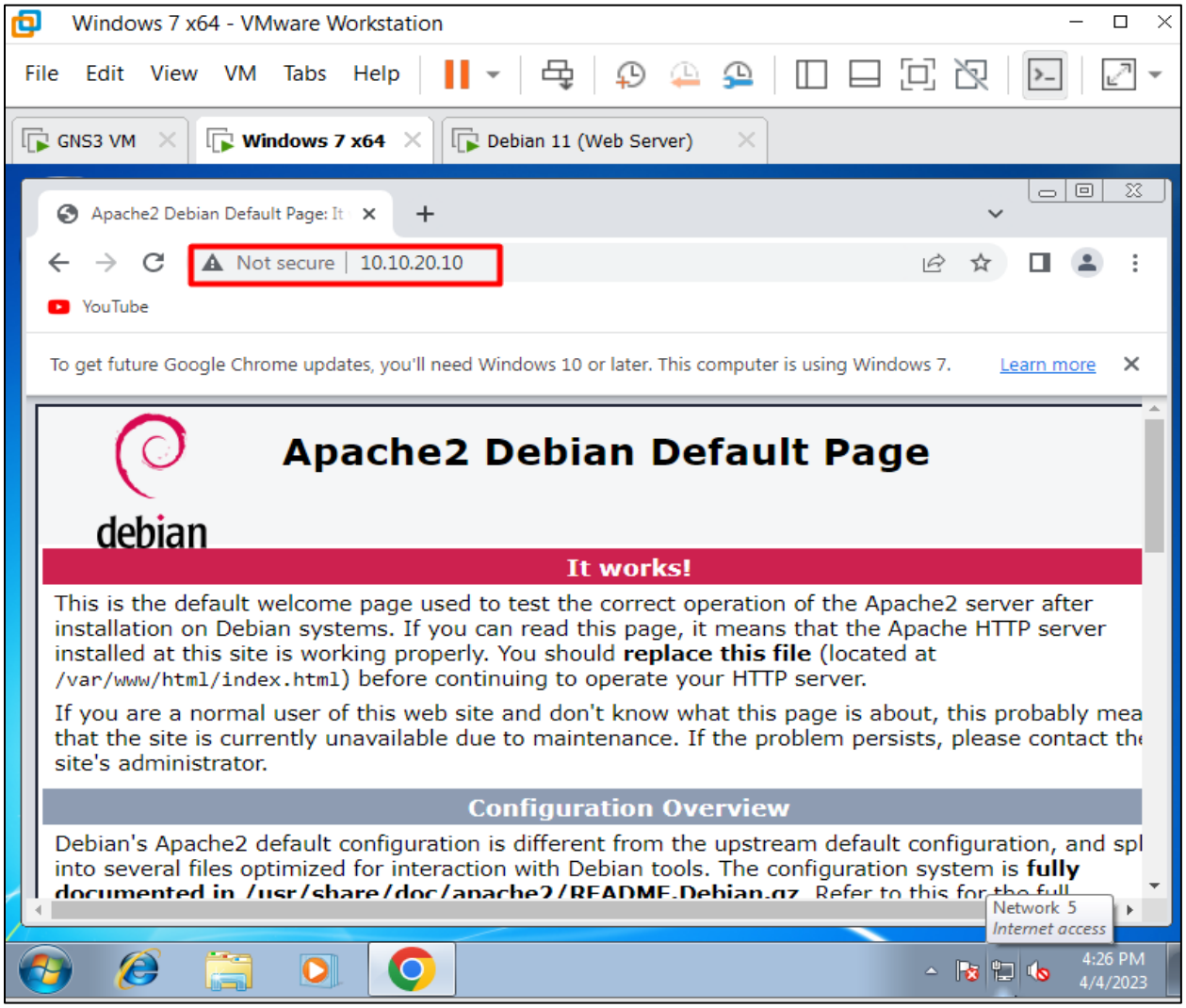


Figure 79 Firewall policy for accessing the web server in DMZ zone from internal network.



80 Test results: The internal users can successfully access the web server in DMZ.

Test case 2	
Objective	To test whether the web server in DMZ is accessible by the external/ internet users.
Action	Using the same virtual IPs, add a firewall policy to access web server in DMZ.
Expected test Result	The default Apache webpage should be displayed after browsing wan interface IP (192.168.70.5).
Actual test result	The default webpage is displayed after browsing wan interface IP (192.168.70.5).
Conclusion	Successfully done. The external/internet users can access web server in DMZ.

Table 32 DMZ test case 2.

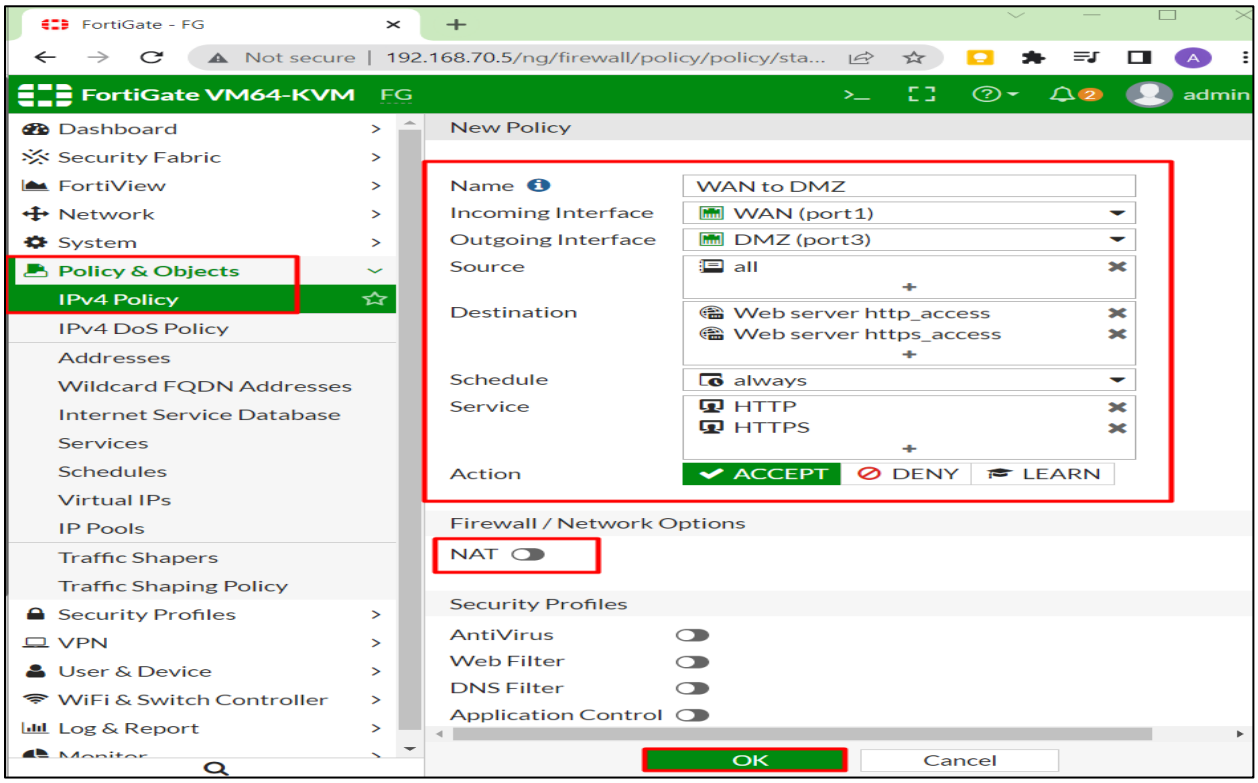


Figure 81 Firewall policy to access the web server in DMZ zone from external network.

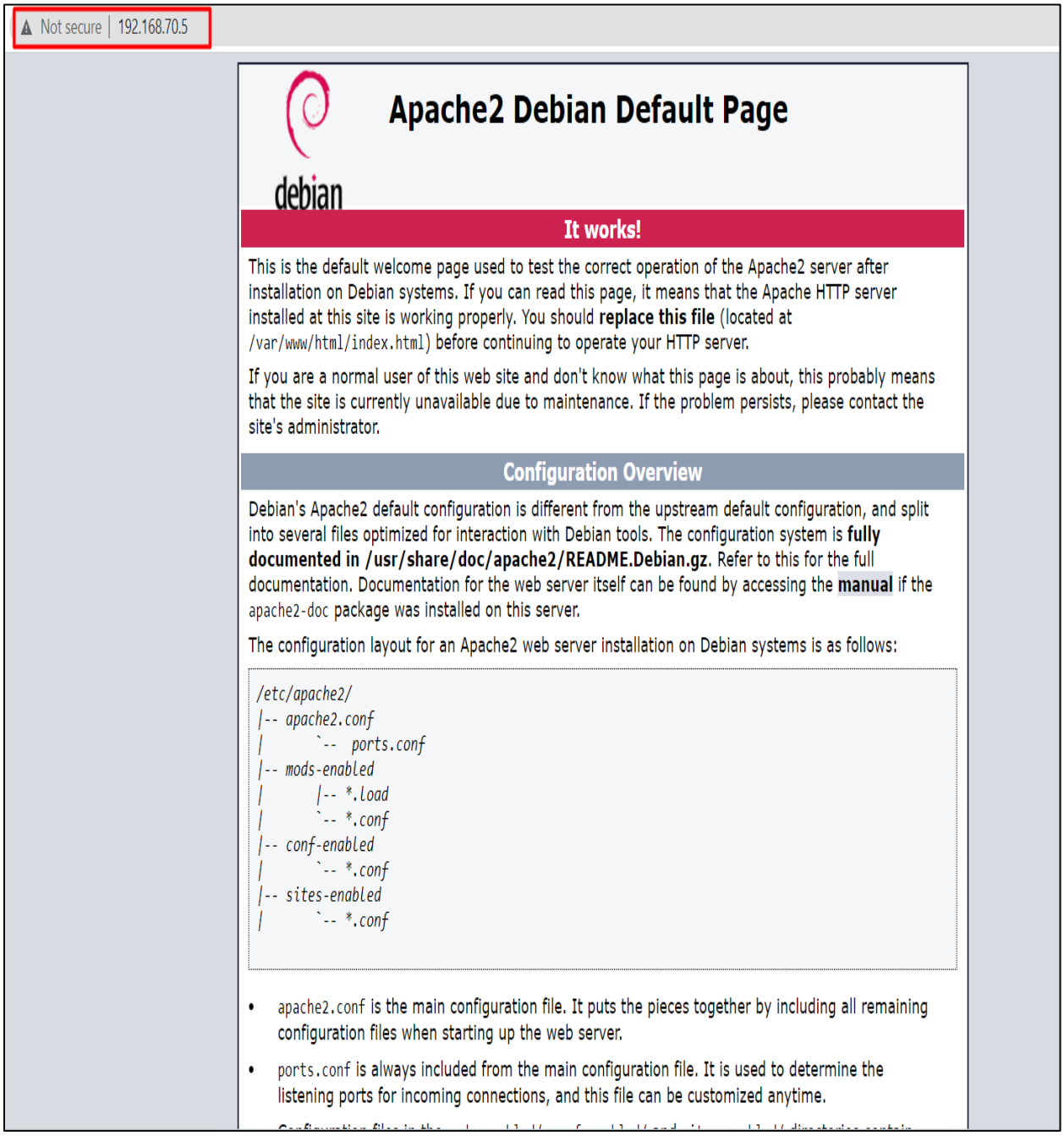


Figure 82 Test results: The internet/external users can successfully access the web server in DMZ.

4.2.2.2. Remote access policies test cases.

Test case 1	
Objective	To test whether the domain controller can remotely access all the users and computer or not.
Action	• Open remote desktop connection. • Enter the IP address of internal web server. • Enter the admin password. • Repeat the same steps for IT department user's computer and other department user's computer.
Expected test Result	The DC (domain controller) should be able to remotely access the server and computers.
Actual test result	The DC is able to remotely access the server and computers.
Conclusion	Successfully done.

Table 33 Remote access policies test case 1.

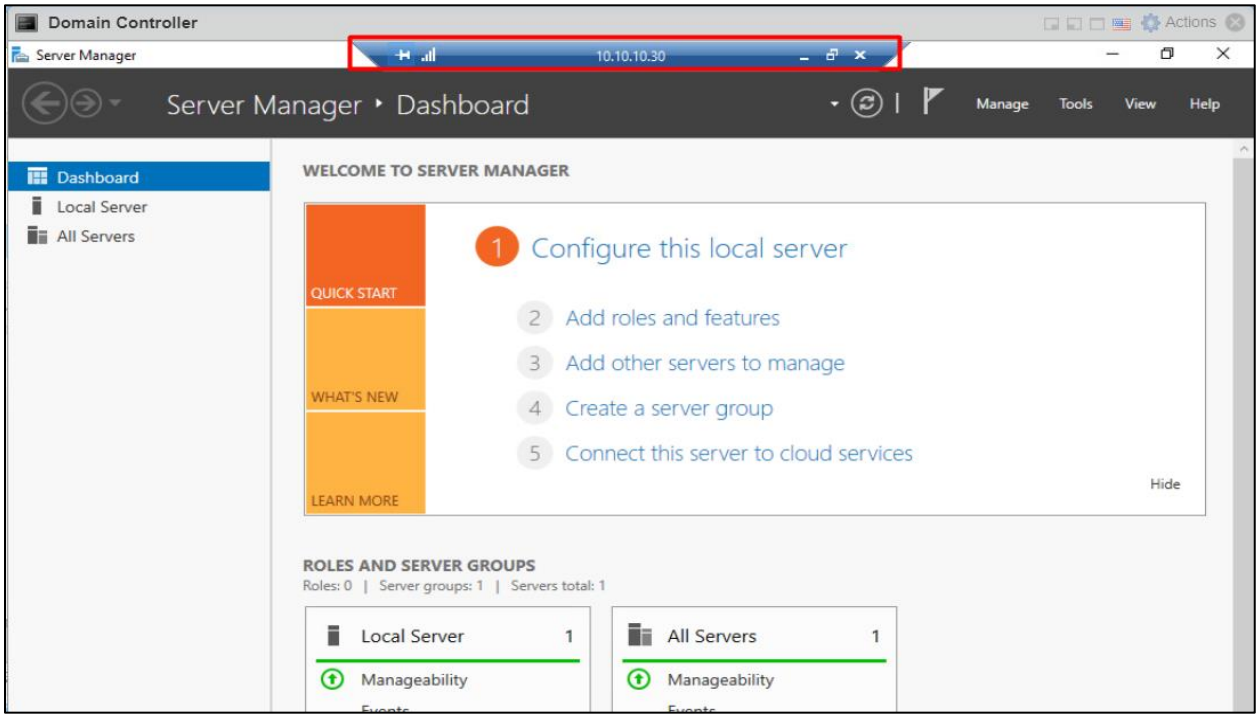


Figure 83Test result: The web server is remotely accessed by DC.

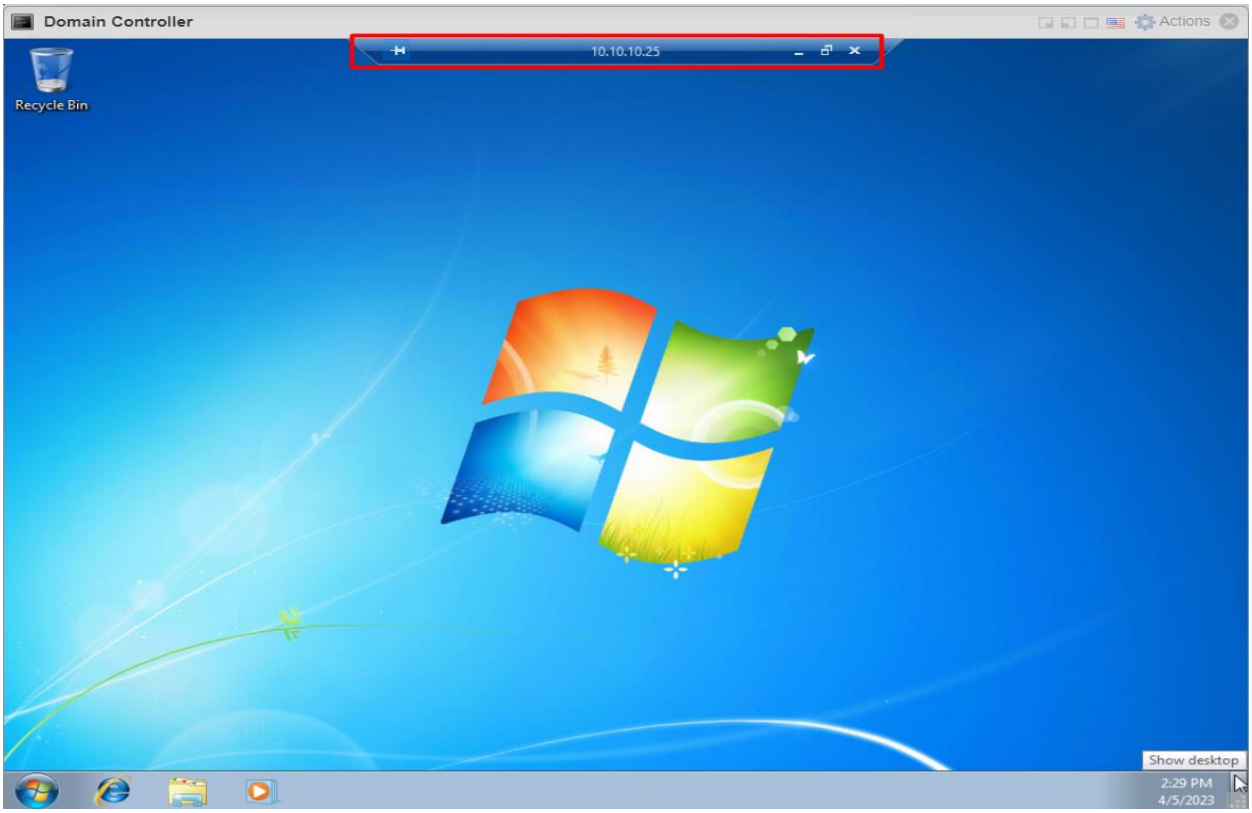


Figure 84 Test result: The CL1 is remotely accessed by DC.

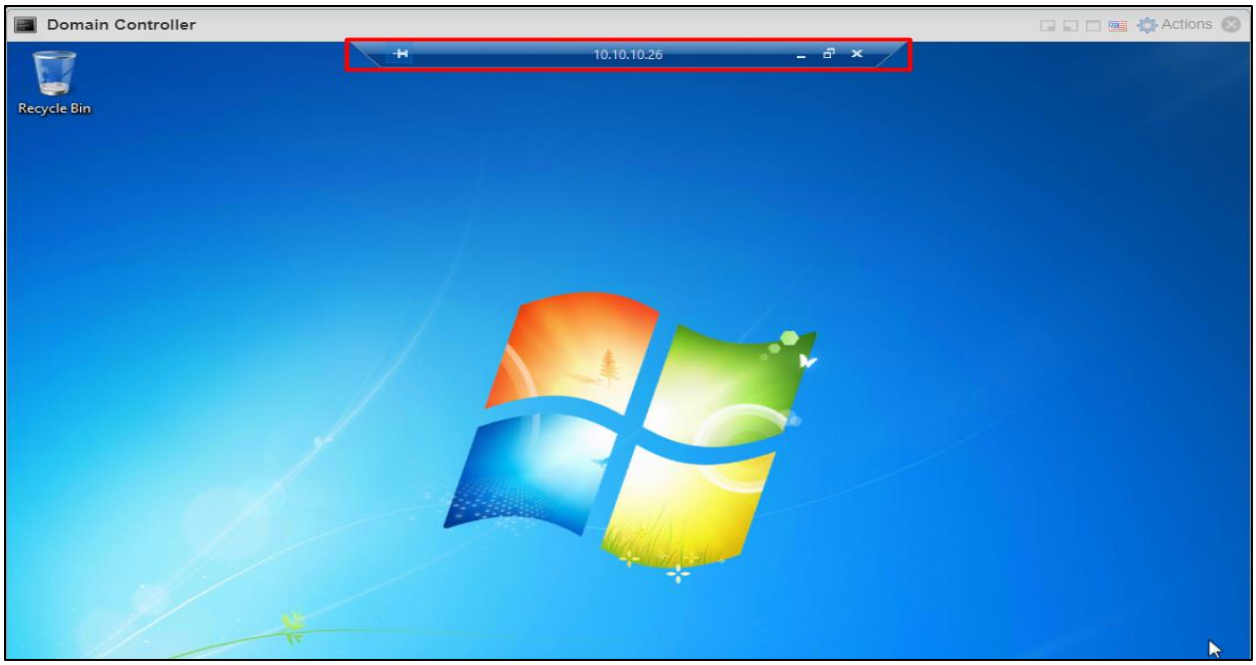


Figure 85 Test result: The CL2 is remotely accessed by DC.

Test case 2	
Objective	To test whether the IT department's employee can remotely access the domain controller or not.
Action	• Add the user in remote access user list. • Open remote desktop connection on IT department user's computer. • Enter the IP address of Domain controller. • Enter the admin password.
Expected test Result	The IT department's user should be able to access DC remotely.
Actual test result	The IT department's user is not able to access DC remotely.
Error	An error message "This computer can't connect to remote computer" is displayed.
Correction	• Edit policies to allow user access the DC remotely (Group policy management>Policies>Windows setting>security setting>Local Policies>User Right Assignment> Allow log on through remote desktop connection> Add user> ok) • Then, add the user to domain admin
Conclusion	Successfully done. The IT user is able to access the DC.

Table 34 Remote access policies test 2.

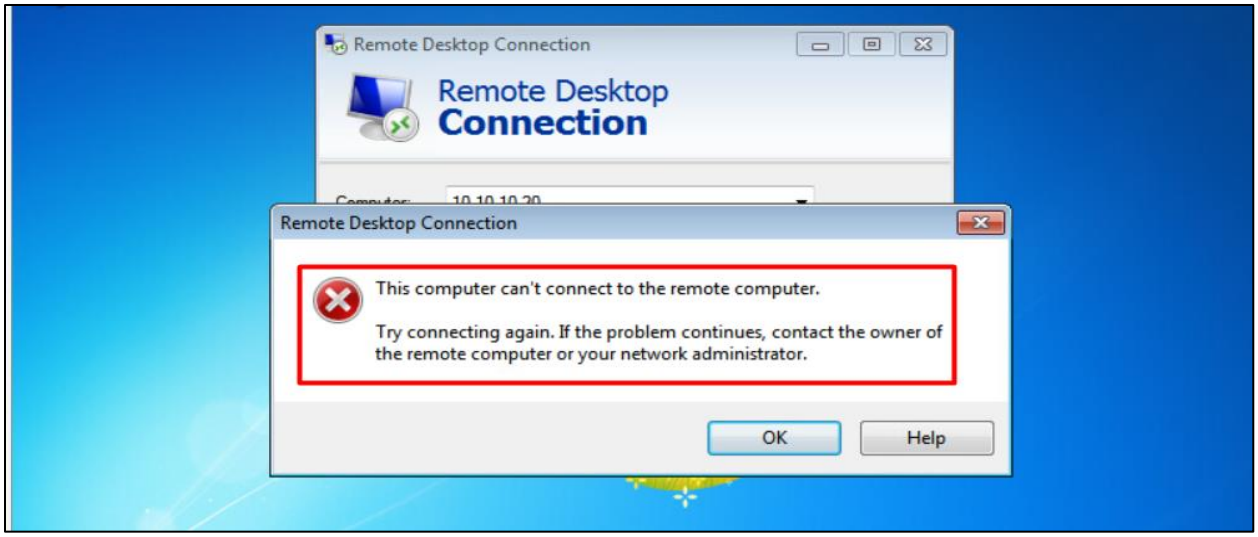


Figure 86 Error of Domain Controller test case 4.

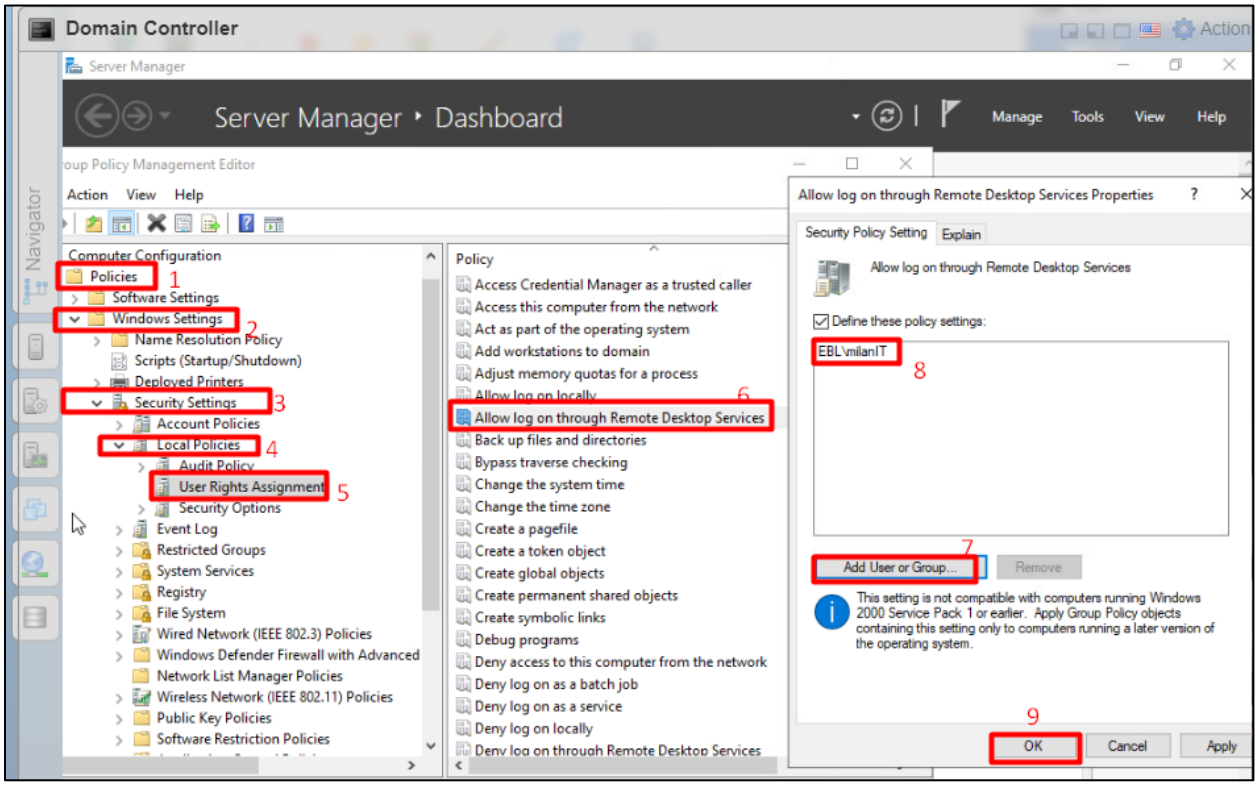


Figure 87 Error correction of Domain Controller test case 4.

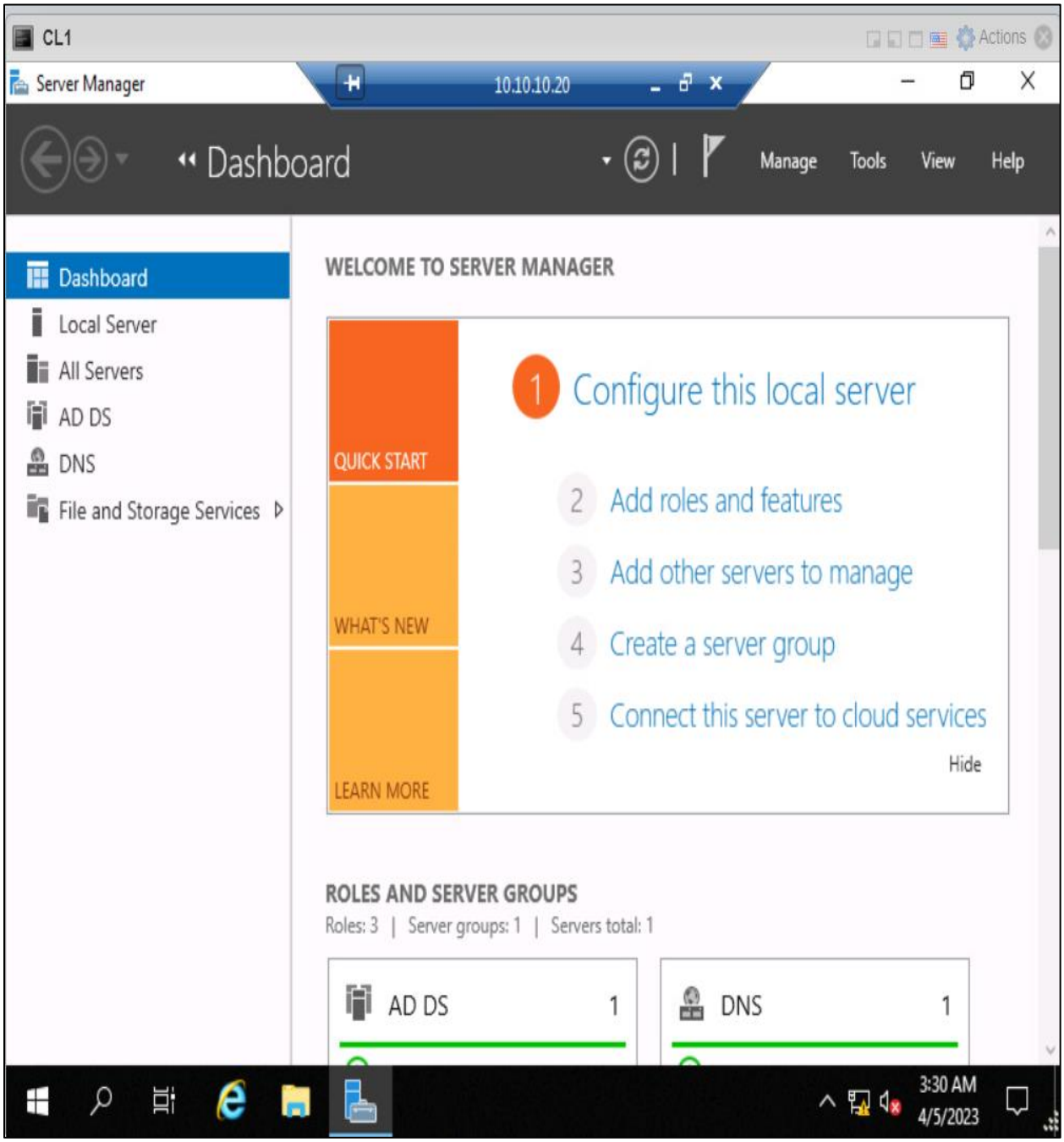


Figure 88 Test result: The user from IT department can access the DC remotely.

Test case 3	
Objective	To test whether the users from other departments can remotely access the DC or not.
Action	• Open remote desktop connection. • Enter the IP address of internal web server. • Enter the admin password.
Expected test Result	The users should not be able to access the DC remotely.
Actual test result	The users are not able to access the DC remotely.
Conclusion	Successfully done.

Table 35 Remote access policies test 3.

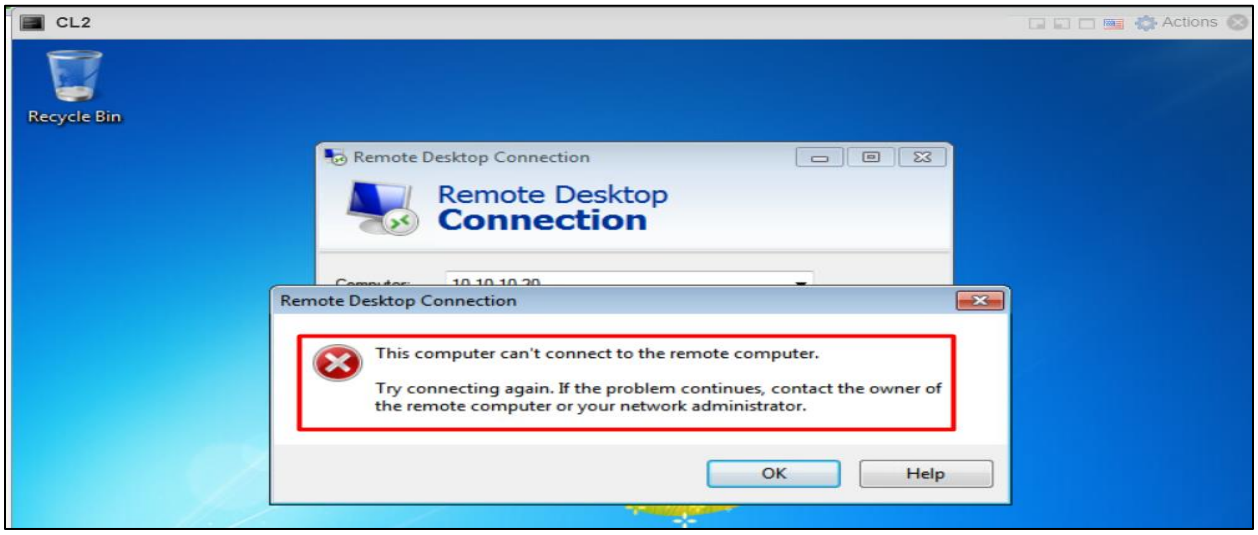


Figure 89 Test result: The user from another department is not able to access DC remotely.

4.2.2.3. Internal website test case.

Test case 1	
Objective	To test internal website is hosted properly or not.
Action	• Open browser and enter the IP address “10.10.10.30”
Expected test Result	A webpage should be displayed.
Actual test result	The web page is displayed
Conclusion	Successfully done.

Table 36 Internal website test case 1

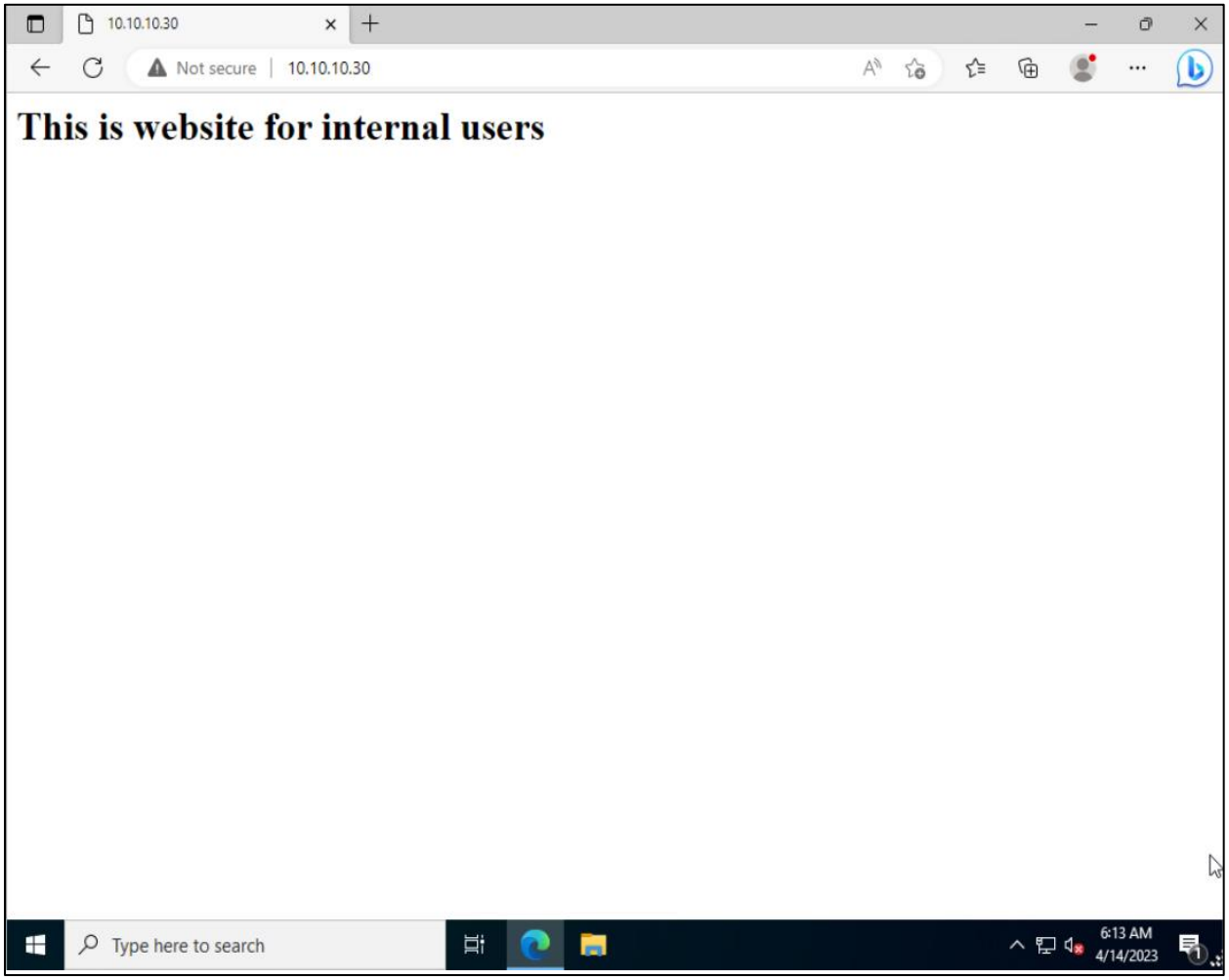


Figure 90 Test result: The internal website is hosted successfully.

4.2.2.4. Asset management test cases.

Test case 1	
Objective	To test whether the LAN sweeper is scanning the assets in the network or not
Action	Select the scan button and start scanning.
Expected test Result	It should display all the software's and assets present in the network.
Actual test result	It displayed all the software's and asset present in the network.
Conclusion	Successfully done.

Table 37 Asset management test case 1

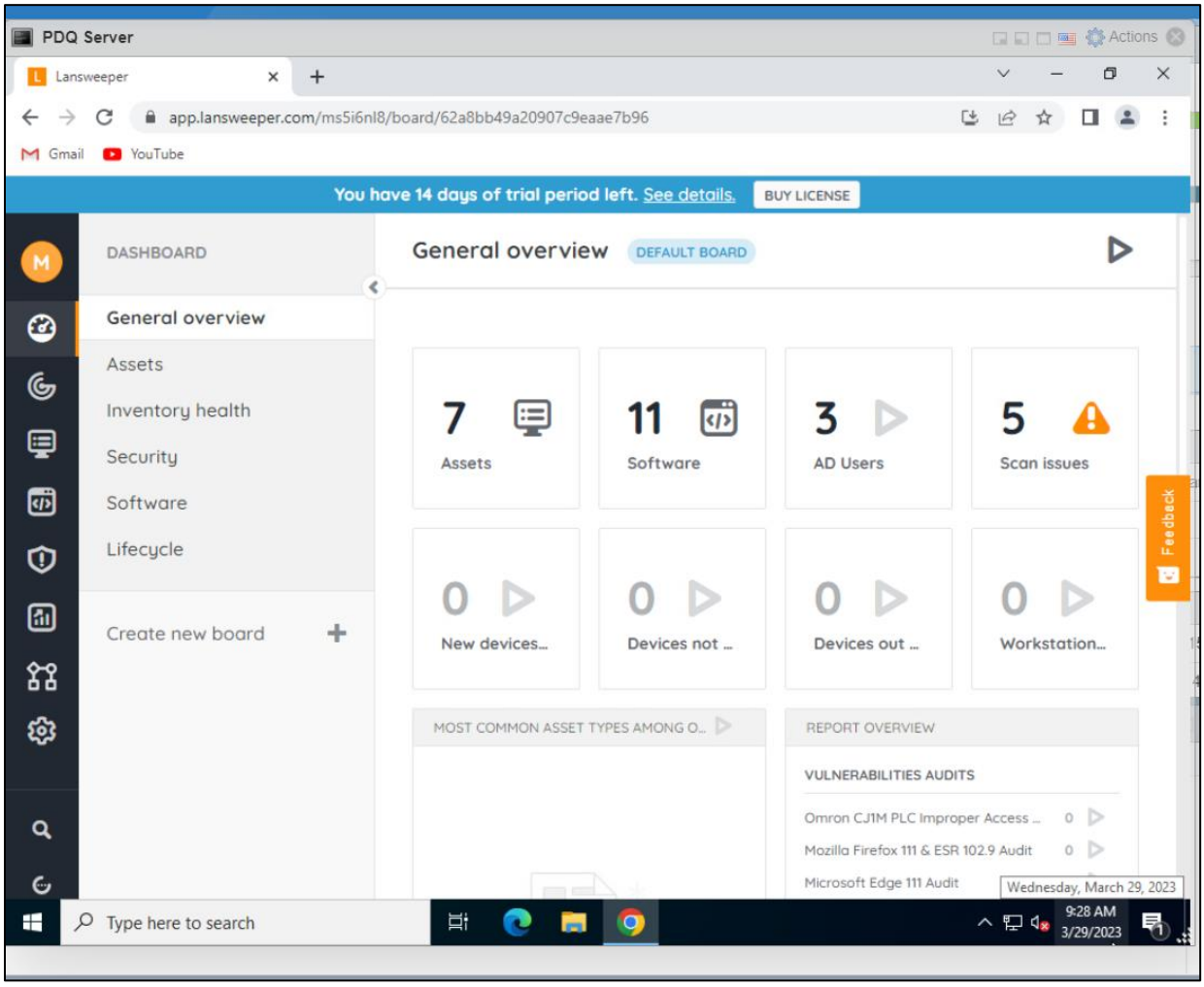


Figure 91 Test result: The LAN sweeper has scanned the assets, software and AD users present in network.

Test case 2	
Objective	To test whether the LAN sweeper is displaying any credentials issue or not.
Action	Select the dashboard button > credential issues button
Expected test Result	It should display all credential issues related to the assets.
Actual test result	It displayed all the credential issues related to the assets.
Conclusion	Successfully done.

Table 38 Asset management test case 1

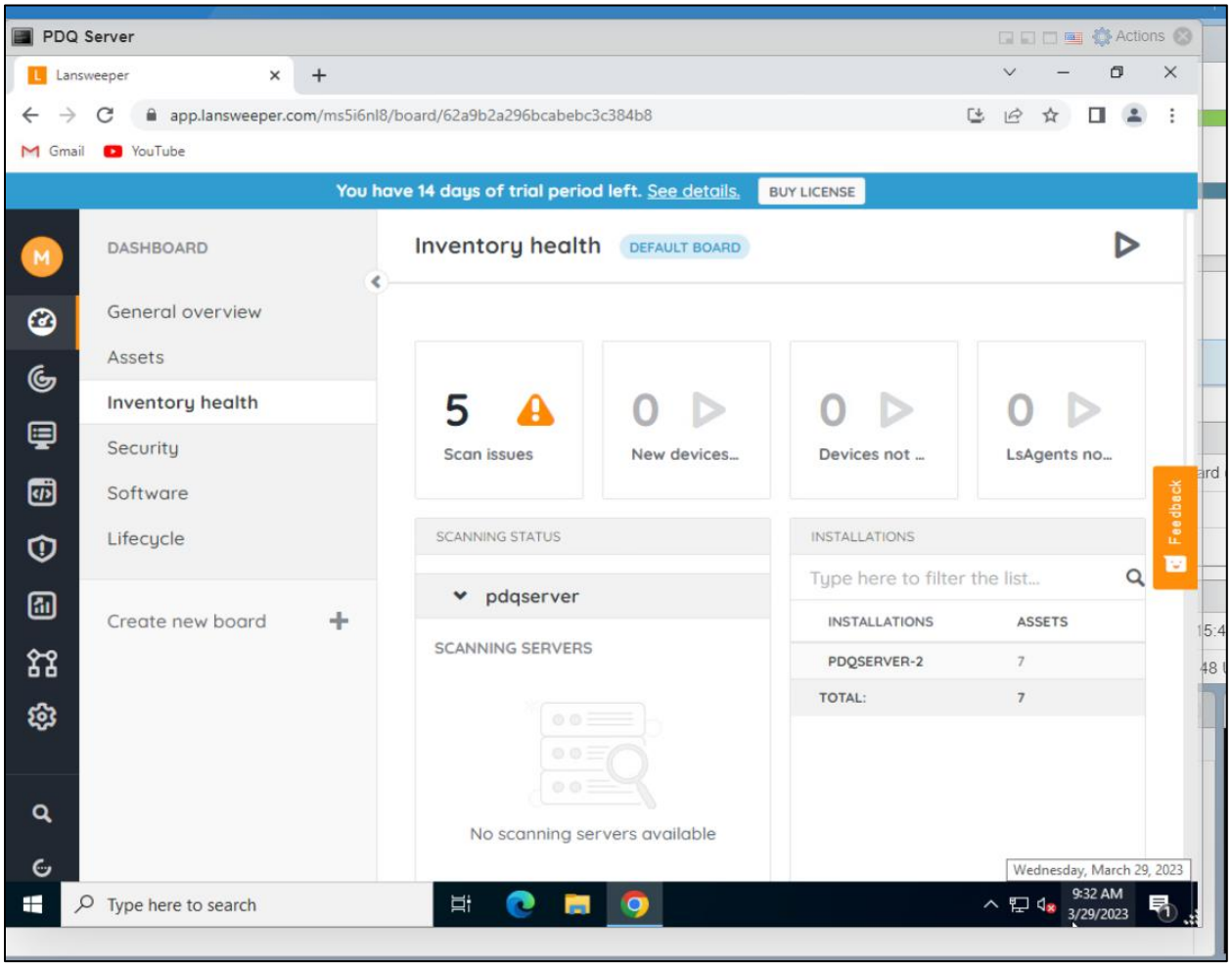


Figure 92 Test results: The LAN sweeper is displaying the credential issues.

4.2.2.5. Software package deployment test cases.

Test case 1	
Objective	To test whether the package is added for deployment or not
Action	• Download the inbuilt package for deployment. • Add in the package list.
Expected test Result	The packages should be added without any errors.
Actual test result	The package is added without any errors.
Conclusion	Successfully done.

Table 39 Software package deployment test case 1.

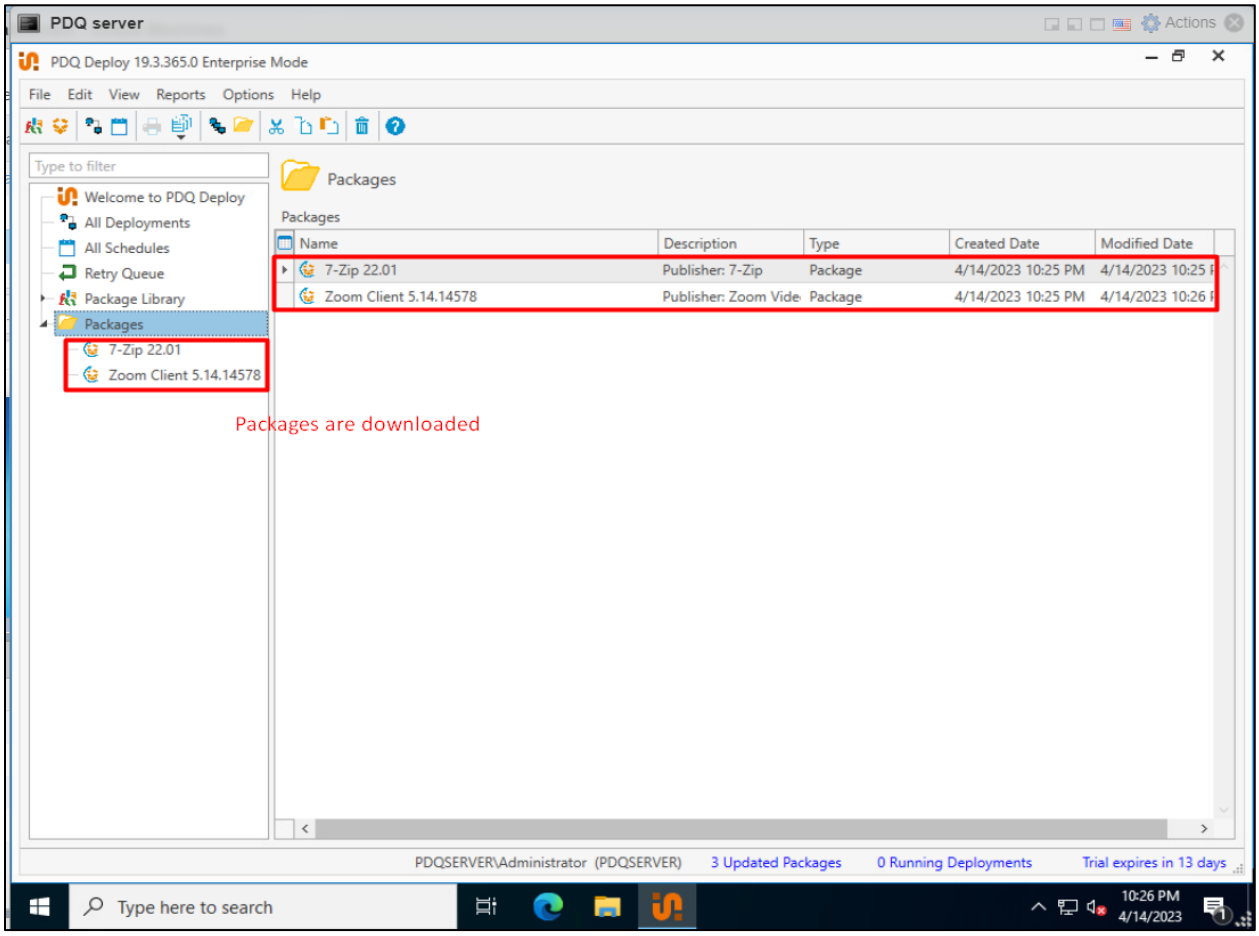


Figure 93 Test result: The package is downloaded successfully.

Test case 2	
Objective	To test manual deployment of the package.
Action	• Choose one of the added packages and select the targets. • Deploy instantly.
Expected test Result	The package should be deployed simultaneously in all targeted computers.
Actual test result	The package is deployed simultaneously in all targeted computers.
Conclusion	Successfully done.

Table 40 Software package deployment test case 2.

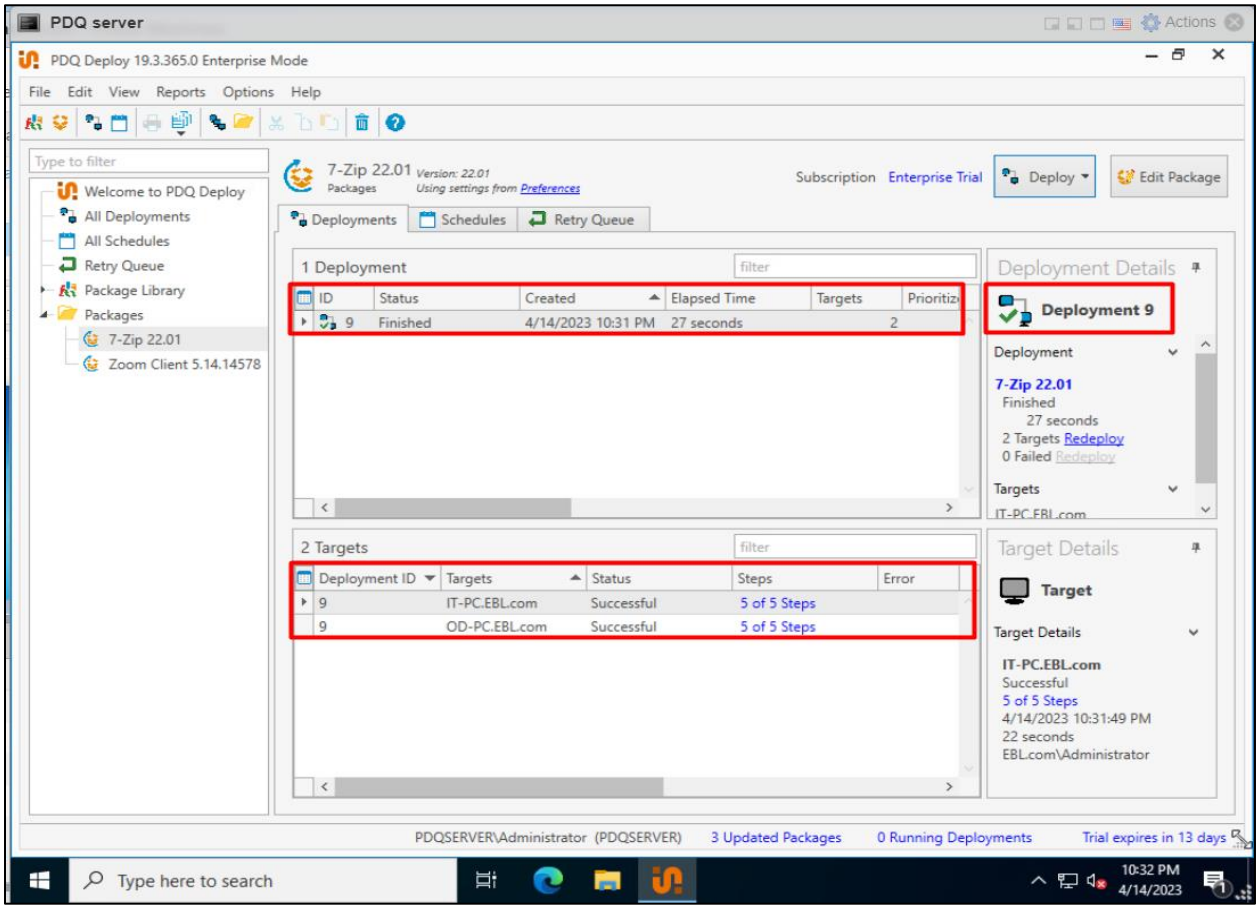


Figure 94 Test Result: The package is deployed simultaneously in all targeted computers.

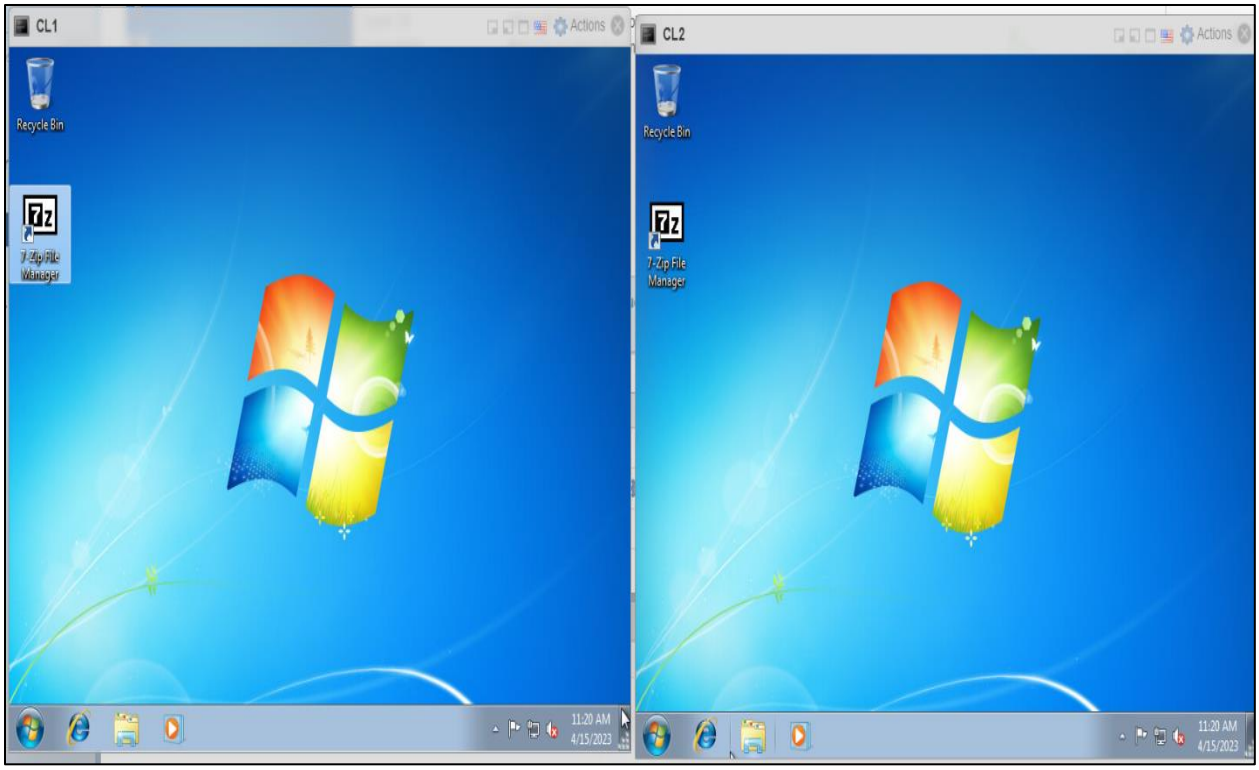


Figure 95 Test Result: Manual package deployment was successful.

Test case 3	
Objective	To test the scheduled and triggered deployment of package.
Action	• Choose the package to be deployed. • Add a desired schedule and targets. • Turn on trigger mode and leave for deployment.
Expected test Result	The deployment should automatically start at scheduled date and time.
Actual test result	The deployment started automatically at the scheduled date and time
Conclusion	Successfully done.

Table 41 Software package deployment test case 1.

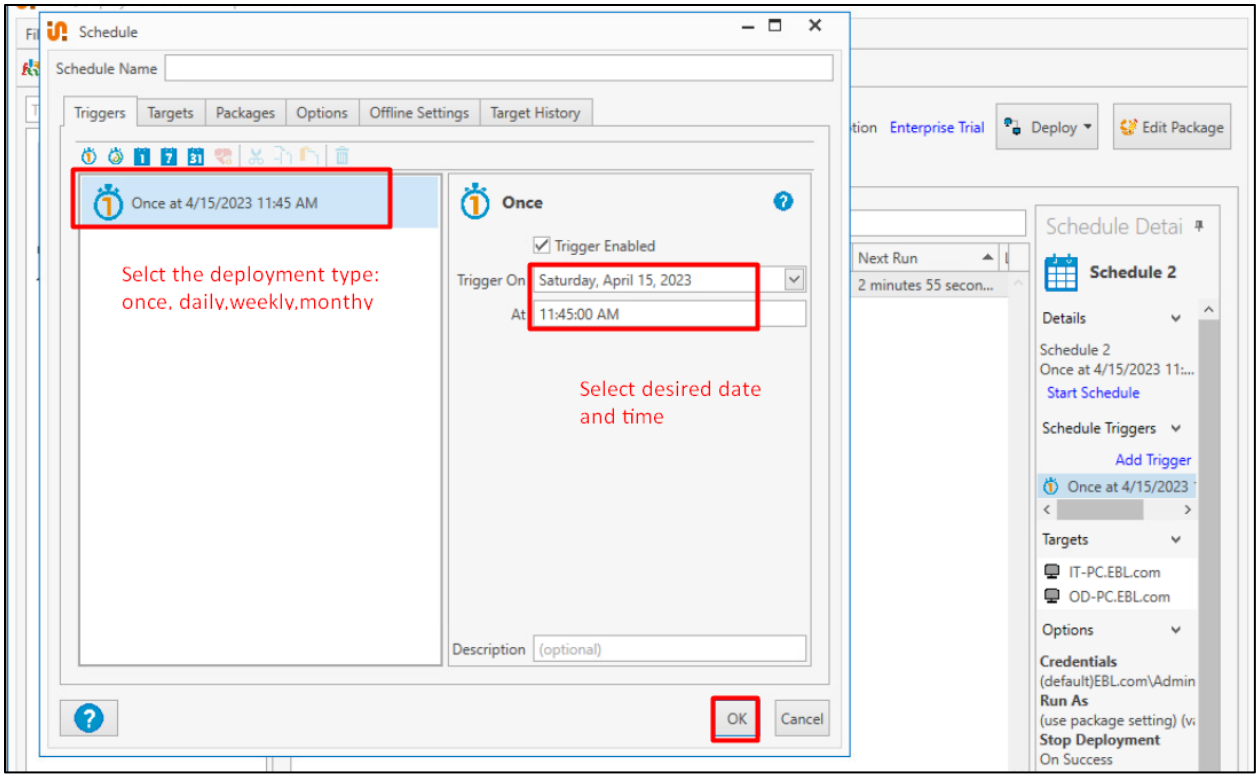


Figure 96 Creating a schedule for automatic package deployment.

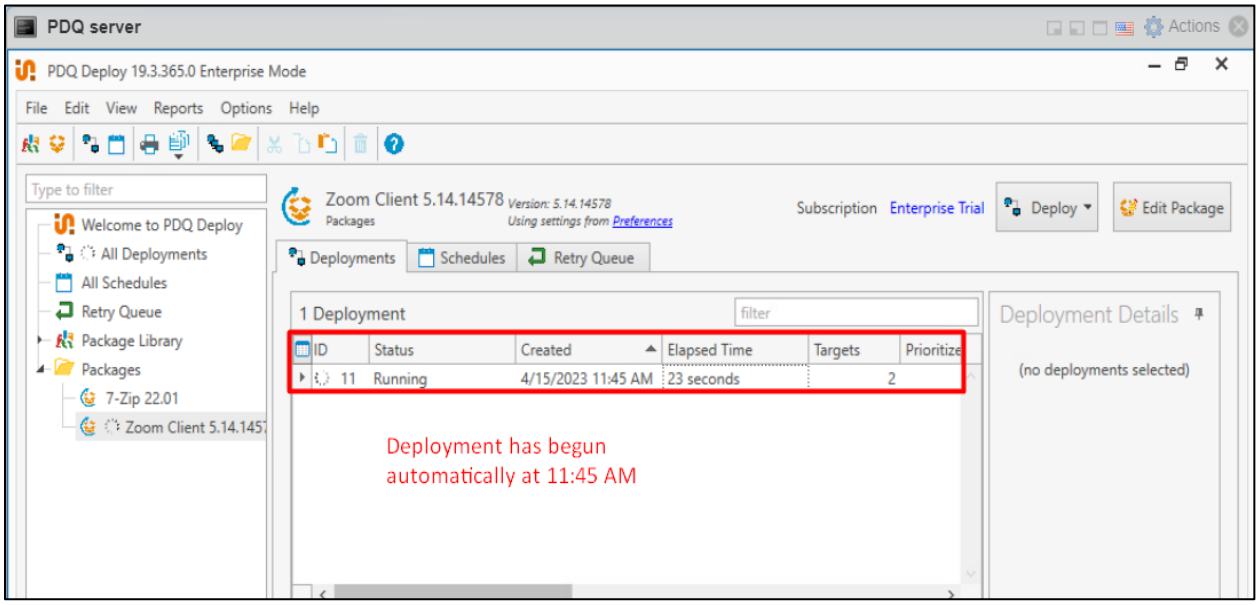


Figure 97 Test result: The package deployment has begun automatically at scheduled time.

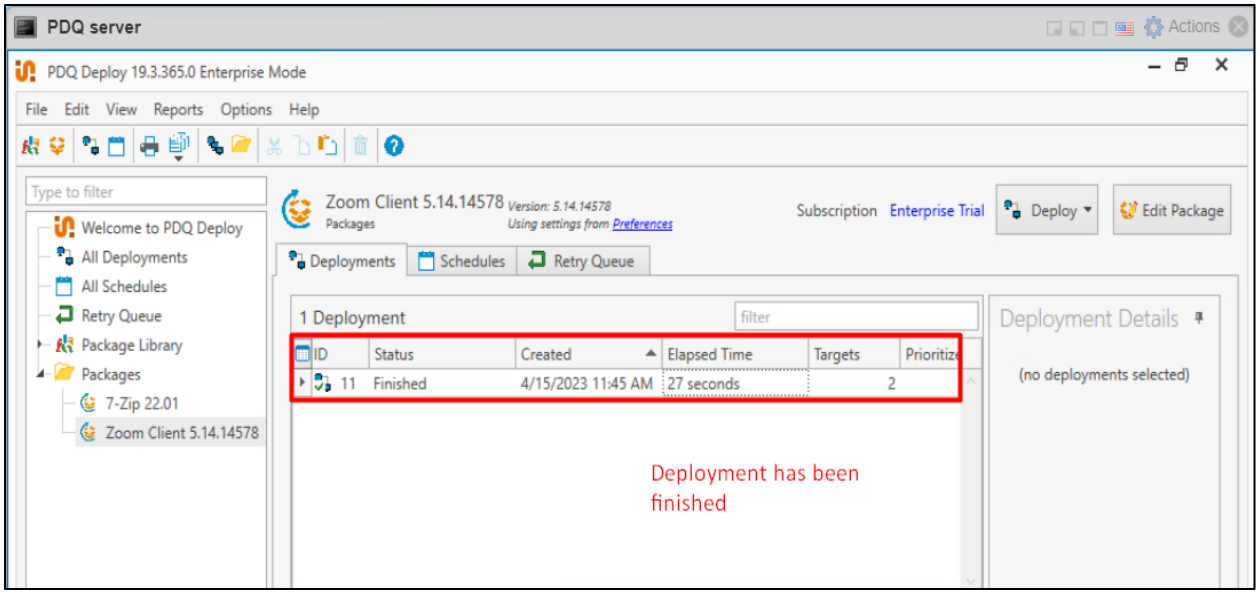


Figure 98 Test result: The package is deployed automatically in all targeted computers.

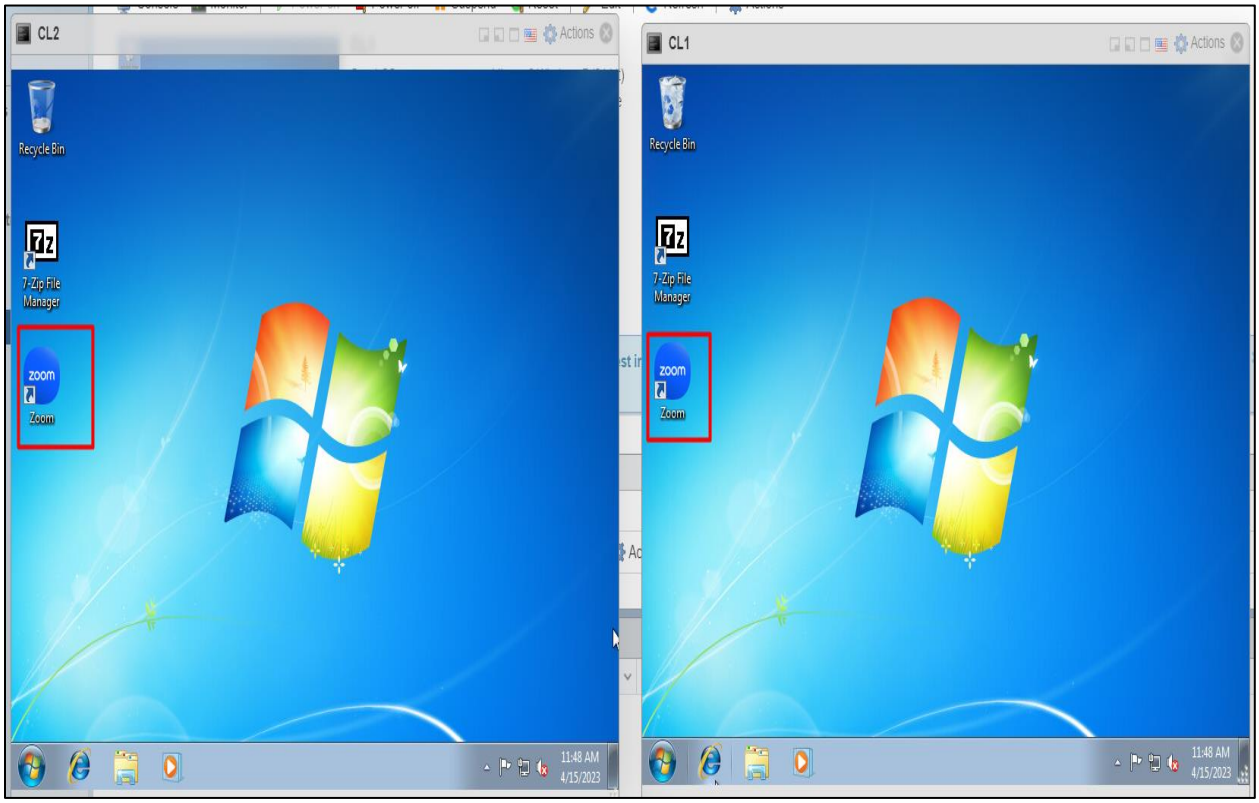


Figure 99 Test result: Scheduled and triggered deployment is successful.

Test case 4	
Objective	To test whether the deployed packages are functional or not.
Action	• Open the computers to which the packages were deployed. • Start the deployed software/application.
Expected test Result	The software/application should function as normal installation.
Actual test result	The software/ application is functional as normal installation.
Conclusion	Successfully done.

Table 42 Software package deployment test case 4.

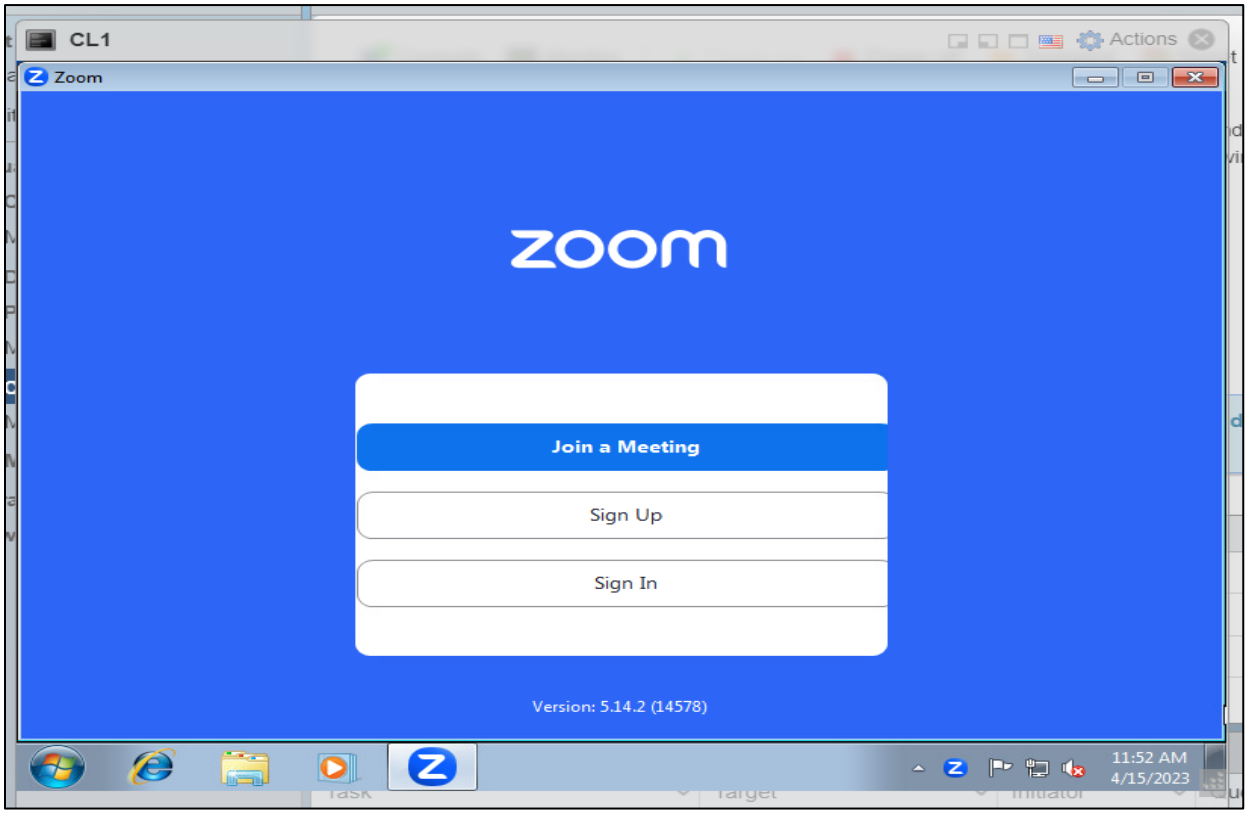


Figure 100 Test result: The deployed package is properly functioning (CL1).

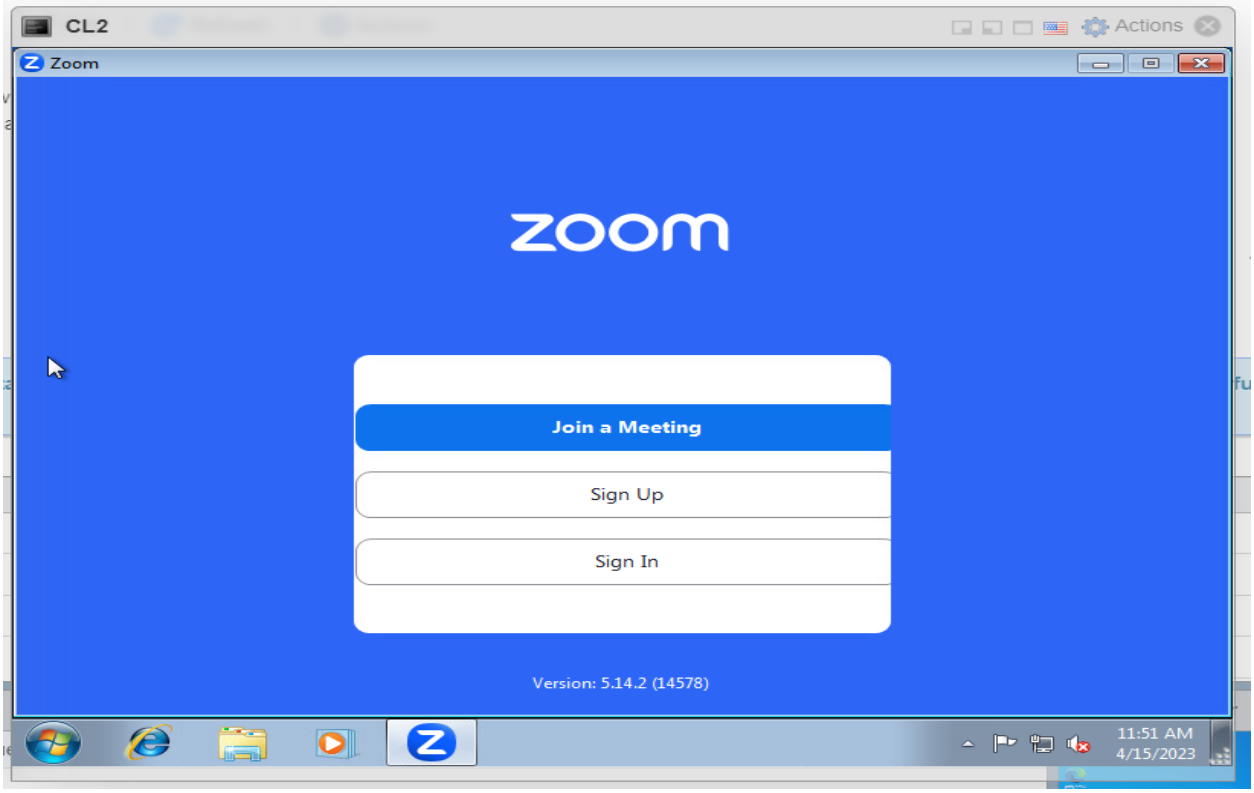


Figure 101 Test result: The deployed package is properly functioning (CL2).

4.3. Critical Analysis

4.3.1. Test summary

There were some extremely challenging problems during the testing phases. However, these problems and errors were identified and rectified, resulting in the successful completion of testing process. The system has been developed by following the evolutionary prototyping methodology. Firstly, an initial system is developed and presented to the client and the final system is built after gathering the feedback and additional requirements of the client. Lastly, the refined system is tested and evaluated, All the test cases mentioned in the test plan section are evaluated with accordance to the requirement of the client and proposed system. This phase proved to be highly beneficial in detecting logical and practical issues that were previously unnoticed, ultimately leading to a more robust and reliable system. Overall, the final system is now fully operational and includes all the features mentioned by the client.

4.3.2. Evaluation

The evaluation of a system is a crucial step in the software development process, as it helps to ensure whether the system meets the intended requirements and operates as expected. The evaluation of the system is done against the main aim and objectives of the system. The main aim of this project is to build a system in a virtual environment that safeguards the internal network of an organization with DMZ implementation, maintains the network elements like user, policies via ADDS, eases the asset scanning and management via LAN sweeper and perform software deployments as well as patch management via PDQ deploy. This project is for those organization that are facing the problems of network threats, centralized management, asset managing issues and time-consuming manual software installation issue.

Further evaluation of the system is given below,

4.3.2.1. Evaluation of project deliverables

The major deliverables of the project were requirement gatherings, system design, system development, test plans, test cases, test results and a final working system. All of these deliverables have been accomplished successfully during this project. So, from the perspective of project deliverables, it can be concluded that the project has been accomplished successfully.

4.3.2.2. System evaluation

All the essential functional requirements and committed features to the client organization have been achieved. The system was developed by leveraging a diverse range of tools and technologies. The system is now able to provide an additional layer of security to internal network with the DMZ implementation on external service providing server. Additionally, the centralized control and management of users and policies can be performed flawlessly sing this system. Moreover, the system is able to perform asset management conveniently in a short time. This system also includes an extra feature i.e., easy software deployment and patch management. All the tasks and milestone were completed as scheduled. This system has solved the problem of the client and other companies who are facing same problems.

CHAPTER 5: CONCLUSION

Today's organizations are facing multitude of challenges, the primary challenge among them is being the rising prevalence of network and cyber threats. Additionally, centralized management of complex network infrastructure and the laborious process of manual package installation are also consuming a lot of time, cost, and effort of the organizations. To overcome these issues, this project was created specifically. As we can see, even most of the organization in Nepal follow the traditional management of network infrastructure such as manual, paper based or spreadsheets. Moreover. The organization are also following the manual software installation such as downloading from internet on each device manually. These methods are prone to error and spend huge efforts and time. This system provides an additional layer of security to the internal network of the organization with the DMZ implementation. Moreover, this system also simplifies the management of network elements and can improve administrative control over the resources. This system on implementation will also eradicate the major headache of the organizations i.e., manual software installation by streamlining software deployment, ensuring that all the software on the system is up-to-date and secure.

Overall, with the successful implementation of these tools, the system is well-positioned to support the needs of modern business, and it represents a significant step forward in the field of enterprise system development.

5.1. Legal, Social, and ethical issues

Considering legal, social, and ethical issues is an essential aspect of project development. It is imperative to take these issues into an account to avoid negative outcomes that may affect the project or its stakeholders. To be precise, this is an educational project meant to be accomplished for the final year of B.Sc. Computer Networking and IT security program, conducted by London Metropolitan University. While developing the project, all the guidelines provided by the Islington college and London metropolitan University has been followed strictly. Thus, ensuring the strict consideration of legal, social, and ethical issues throughout the research, information gathering, development and report writing processes.

5.1.1. Legal issues

The issues caused by violating the laws and regulations are legal issues. The legal issues that may arise while developing a virtualized system can include software licensing agreements, intellectual property rights, data protection and privacy and so on (Dudley, et al., 2023).

Regarding this project, the software utilized in the development of the system comprises both student versions as well as trial versions. Meanwhile, the other software used in this project are preowned by me. This project does not have any legal issues since every task has been carried out in a virtual machine, not affecting any real time networks or users. To be precise, the laws has been strictly considered while gathering the information and accessing the networks.

5.1.2. Social issues

Social issues are the problems that affect the well-being of individuals or a society. In this project, all the assembled information has been evaluated fairly. The content of the project includes beneficial and acceptable information that positively impacts the individual and group of the society. Moreover, the project does not delve into religiously and politically inclined topics. Thus, ensuring complete absence of any social issues in this project.

5.1.3. Ethical issues

Ethical issues are the concerns about what is morally acceptable and unacceptable in a specific situation. The client of this project is Everest Bank Limited (EBL). Regarding this project, all the permits for information gatherings were conveniently obtained. Moreover, all the meetings and data collection were carried out with the client's consent and permission. Considering the plagiarism, the research and the report has been thoroughly referenced, leaving no uncertainty. Overall, this project complies entirely with the rules and regulations set by London Metropolitan University and all the work carried out has not violated the intellectual property rights of the client or any authors and researchers whose work has been referenced.

5.2. Advantages

Some of the advantages of this system are given below,

5.2.1. Automated software package deployment

The traditional installation of software package in each computer manually have been a major headache to almost every organization. Use of the PDQ deploy tool eases the software package deployment saving time and effort. This system even won't need an admin to click manual start. The package automatically starts deploying at the scheduled time itself.

5.2.2. Time saving

Since, there is no need for manual asset listing and management, issue identification and software package deployments, time and effort can be saved which can further implemented for other important tasks.

5.2.3. Cost-effective

The system is implemented in virtual environment thus resulting in lower costs for hardware, maintenance, and energy consumption. It also improves the overall efficiency and performance of the system. Additionally, this system allows greater flexibility in resource allocation, enabling to allocate more resources as per requirements eventually being cost-effective (Powell, 2022).

5.2.4. Increased security

The DMZ implementation on external server and domain controller internal network has eventually resulted improvements in system's security. Furthermore, the use of network devices of different vendors also has enhanced the system's security (Zavadsky, 2022).

5.2.5. Easy scalability

This system allows easy scalability and manageability of resources and features according to specific need such as scalability of RAM, processors, and other aspects, resulting in high availability to adapt to recent changes.

5.3. Limitations

Like any other endeavor, every system/project has its own features and limitations. Some of the limitations of this project are,

- Trial versions of the software restrict their usage after a certain period.
- To use this product, someone must have knowledge of virtualization.
- The system configuration and demonstration require a computer with a processor that has a minimum of 16 GB RAM capacity to run properly.
- The estimated budget may not be sufficient as this system is always available for changes and additional features.
- There is not much assistance/ guide.
- The functionality of the system can be impacted by unintentional change of the settings/configuration.

5.4. Future work

Though all the client requirements are fulfilled, this system can further be enhanced by implementing things which are listed below,

- Disaster recovery planning

  The system can be improved to include disaster recovery planning, including proper backup restoration procedures to ensure quick data recovery outages.

- Active Directory enhancements

  The domain controller can be improved to better manage users and devices within the system, including the implementation of group policies, centralized authentication, and auditing.

- Security improvements

  The system's security measures can be further enhanced by implementing additional security controls, such as ACL, IDS/IPS etc.

- Performance optimization

  The system's performance can be optimized by upgrading hardware components.

- Automated asset management

  The paid version of Lansweeper includes automated actions that can be triggered based on specific events or conditions allowing more efficient and proactive management of network assets.

- Scripted software package deployments.

  The PDQ deploy allows package customization. The packages can be customized using PowerShell, batch files and other scripting languages allowing administrators to deploy self-built packages.

CHAPTER 6. REFERENCES

Afreen, S., 2023. *VMware Workstation: Everything You Need to Know*. [Online] Available at: https://www.simplilearn.com/tutorials/cloud-computing-tutorial/vmware-workstation
[Accessed 10 04 2023].

Agelica, L., 2023. *Types of Prototypes: Which is best for Your Design.* [Online] Available at: https://mockitt.wondershare.com/prototyping/types-of-prototype.html [Accessed 15 04 2023].

Alsaquor, R., Motmi, A. & Abdelhaq, M., 2021. A Systematic Study of Network Firewall and Its Implementation. *International Journal of Computer Science and Network Security,* 21(4), pp. 199-207.

Ayuya, C., 2023. *What is Patch Management?.* [Online] Available at: https://www.esecurityplanet.com/networks/patch-management/ [Accessed 17 04 2023].

Bagci, T., 2022. *What is GNS3? | What Does it Do?.* [Online] Available at: https://www.sysnettechsolutions.com/en/what-is-gns3/ [Accessed 10 04 2023].

BANGER, E. R. S., 2023. *What is Debian? Advantages and Disadvantages | Debian Features.* [Online]
Available at: https://digitalthinkerhelp.com/what-is-debian-advantages-disadvantages/ [Accessed 16 04 2023].

Barney, N., 2022. *network security.* [Online] Available at: https://www.techtarget.com/searchnetworking/definition/network-security [Accessed 30 03 2023].

BasuMallick, C., 2022. *What Is a Demilitarized Zone (DMZ)? Definition, Examples, Working, and Importance in 2022.* [Online] Available at: https://www.spiceworks.com/it-security/network-security/articles/what-is-

demilitarized-zone/
[Accessed 30 03 2023].

Bender, J., 2023. *What Is Windows Server and How Can Businesses Use It?*. [Online] Available at: https://www.businessnewsdaily.com/windows-server [Accessed 16 04 2023].

Bermejo, B., Juiz, C. & Guerrero, c., 2019. Virtualization and consolidation: a systematic review of the past 10 years of research on energy and performance. *The journal of supercomputing,* 75(2), pp. 808-836.

Braden, A., 2021. *VMWare Workstation.* [Online] Available at: https://www.webopedia.com/definitions/vmware-workstation/ [Accessed 10 04 2023].

Chouffani, R., 2023. *IT asset management (ITAM).* [Online] Available at: https://www.techtarget.com/searchcio/definition/IT-asset-management-information-technology-asset-management
[Accessed 15 04 2023].

clearfind, 2023. *What is PDQ deploy?.* [Online] Available at: https://clearfind.com/guides/products/pdq-deploy [Accessed 05 04 2023].

Collegenote, 2018. *Why an evolutionary prototyping is used in software development? Explain..* [Online]
Available at: https://www.collegenote.net/pastpapers/4420/question/ [Accessed 30 03 2023].

CyberHoot, 2020. *Demilitarized Zone (DMZ).* [Online] Available at: https://cyberhoot.com/cybrary/demilitarized-zone-dmz/ [Accessed 30 03 2023].

Debian.org, 2023. *Debian 11 bullseye.* [Online] Available at: https://www.debian.org/News/2021/20210814 [Accessed 10 04 2023].

Deshpande, C., 2022. *What Is Firewall: Types, How Does It Work, Advantages & Its Importance.* [Online]
Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall
[Accessed 15 04 2023].

Dudley, A., Braman , J., Wang, K. & Vincenti, G., 2023. *Security, Legal, and Ethical Implications of Using Virtual Worlds.* [Online]
Available at: https://www.researchgate.net/publication/228968768_Security_Legal_and_Ethical_Implications_of_Using_Virtual_Worlds
[Accessed 10 04 2023].

Everest Bank Limited, 2023. *Everest Bank Limited.* [Online]
Available at: https://everestbankltd.com/
[Accessed 30 03 2023].

Feilz, F., 2022. *What is VMware ESXi?.* [Online]
Available at: https://www.liquidweb.com/kb/what-is-vmware-esxi/
[Accessed 15 04 2023].

Fisher, T., 2021. *What Is a Router and How Does It Work?.* [Online]
Available at: https://www.lifewire.com/what-is-a-router-2618162
[Accessed 15 04 2023].

Gantt Project, 2023. *Free desktop project management software.* [Online]
Available at: https://www.ganttproject.biz/
[Accessed 10 04 2023].

GNS3, 2023. *Getting Started with GNS3.* [Online]
Available at: https://docs.gns3.com/docs/#:~:text=GNS3%20is%20used%20by%20hundreds,even%20hosted%20in%20the%20cloud.
[Accessed 10 04 2023].

gns3, 2023. *Which emulator should I use?.* [Online] Available at: https://docs.gns3.com/docs/emulators/which-emulators-should-i-use/ [Accessed 10 04 2023].

Gowda, T., Vanishree, S., MS, V. & K, Y., 2021. OVERVIEW OF VIRTUALIZATION IN CLOUD COMPUTING. *International Research Journal of Modernization in Engineering Technology and Science* , 03(07), pp. 1841-1846.

Grant, M., Khartit, K. & Kazel, M., 2022. *Gantt Charting: Definition, Benefits, and How They're Used.* [Online] Available at: https://www.investopedia.com/terms/g/gantt-chart.asp [Accessed 10 04 2023].

Hamilton, T., 2023. *Agile Methodology: What is Agile Model in Software Testing?.* [Online] Available at: https://www.guru99.com/agile-scrum-extreme-testing.html [Accessed 30 03 2023].

Kennedy, B., 2023. *Lansweeper pros and cons.* [Online] Available at: https://www.peerspot.com/products/lansweeper-pros-and-cons [Accessed 30 03 2023].

Leeron Hoory, C. B., 2022. *What Is Waterfall Methodology? Here's How It Can Help Your Project Management Strategy.* [Online] Available at: https://www.forbes.com/advisor/business/what-is-waterfall-methodology/ [Accessed 16 03 2023].

Martinez, P., 2023. *What is Evolutionary Prototype?.* [Online] Available at: https://mockitt.wondershare.com/prototyping/evolutionary-prototyping.html [Accessed 30 03 2023].

Mohanan, R., 2022. *DevOps vs. Agile Methodology: Key Differences and Similarities.* [Online] Available at: https://www.spiceworks.com/tech/devops/articles/devops-vs-agile/ [Accessed 30 03 2023].

Nepal News, 2023. *8 arrested for hacking bank accounts using mobile apps.* [Online] Available at: https://nepalnews.com/s/capital/8-arrested-for-hacking-bank-accounts-using-

mobile-apps
[Accessed 30 03 2023].

Patel, M., 2020. *Demilitariz Demilitarized Zone: An Ex one: An Exceptional La ceptional Layer of Network Security t er of Network Security to.* [Online] Available at: https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=9311&context=etd [Accessed 15 03 2023].

Powell, R., 2022. *Advantages and Disadvantages of Virtualization.* [Online] Available at: https://circleci.com/blog/top-6-benefits-of-virtualization/ [Accessed 10 04 2023].

Prasain, K., 2022. *The Kathmandu Post.* [Online] Available at: https://kathmandupost.com/money/2022/12/21/nepal-ranks-way-down-in-digital-entrepreneurship-and-innovation
[Accessed 30 03 2023].

Pratik Ragnarson, N. G., 2018. *Firewall implementation and testing.* [Online] Available at: https://www.ida.liu.se/~TDDD17/oldprojects/2009/projects/012-2.pdf [Accessed 15 03 2023].

Rouse, M., 2020. *What Does Microsoft Office Mean?.* [Online] Available at: https://www.techopedia.com/definition/20737/microsoft-office [Accessed 15 04 2023].

Sharma, R. D., 2017. *Nepali banks 'not prepared' to ward off cyber threats.* [Online] Available at: https://kathmandupost.com/money/2017/10/25/nepali-banks-not-prepared-to-ward-off-cyber-threats
[Accessed 30 03 2023].

Shrimali, S., 2017. DeMilitarized Zone: Network Architecture for Information Security. *International Journal of Computer Applications (0975 – 8887),* 174(5), pp. 16-19.

Singh, A., 2022. *What Is A Network Switch And Its Types.* [Online] Available at: https://www.shiksha.com/online-courses/articles/network-switch-and-its-types/ [Accessed 15 04 2023].

UKessays, 2019. *Waterfall Methodology in Software Development.* [Online] Available at: https://www.ukessays.com/essays/computer-science/waterfall-methodology-in-software-development.php
[Accessed 30 03 2023].

Westland, J., 2022. *Scrum Methodology: Roles, Events & Artifacts.* [Online] Available at: https://www.projectmanager.com/blog/scrum-methodology
[Accessed 30 03 2023].

Willlians, E., 2022. *How to Deploy Software with PDQ Deploy - Updated.* [Online] Available at: https://pdf.wondershare.com/business/how-to-deploy-software-with-pdq-deploy.html
[Accessed 15 04 2023].

Zaharia, A., 2023. *300+ Terrifying Cybercrime and Cybersecurity Statistics (2023 EDITION).* [Online]
Available at: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[Accessed 30 03 2023].

Zavadsky, V., 2022. *DMZ Network: How It Works, Its Uses, and Benefits in Network Security.* [Online]
Available at: https://www.linkedin.com/pulse/dmz-network-how-works-its-uses-benefits-security-valdemar-z%C3%A1vadsk%C3%BD
[Accessed 13 04 2023].

CHAPTER 7: BIBLIOGRAPHY

Bibliography

Afreen, S., 2023. *VMware Workstation: Everything You Need to Know*. [Online] Available at: https://www.simplilearn.com/tutorials/cloud-computing-tutorial/vmware-workstation
[Accessed 10 04 2023].

Agelica, L., 2023. *Types of Prototypes: Which is best for Your Design.* [Online] Available at: https://mockitt.wondershare.com/prototyping/types-of-prototype.html
[Accessed 15 04 2023].

Alsaquor, R., Motmi, A. & Abdelhaq, M., 2021. A Systematic Study of Network Firewall and Its Implementation. *International Journal of Computer Science and Network Security,* 21(4), pp. 199-207.

Ayuya, C., 2023. *What is Patch Management?.* [Online] Available at: https://www.esecurityplanet.com/networks/patch-management/
[Accessed 17 04 2023].

Bagci, T., 2022. *What is GNS3? | What Does it Do?.* [Online] Available at: https://www.sysnettechsolutions.com/en/what-is-gns3/
[Accessed 10 04 2023].

BANGER, E. R. S., 2023. *What is Debian? Advantages and Disadvantages | Debian Features.* [Online]
Available at: https://digitalthinkerhelp.com/what-is-debian-advantages-disadvantages/
[Accessed 16 04 2023].

Barney, N., 2022. *network security.* [Online] Available at: https://www.techtarget.com/searchnetworking/definition/network-security
[Accessed 30 03 2023].

BasuMallick, C., 2022. *What Is a Demilitarized Zone (DMZ)? Definition, Examples, Working, and Importance in 2022.* [Online]

Available at: https://www.spiceworks.com/it-security/network-security/articles/what-is-demilitarized-zone/
[Accessed 30 03 2023].

Bender, J., 2023. *What Is Windows Server and How Can Businesses Use It?.* [Online] Available at: https://www.businessnewsdaily.com/windows-server
[Accessed 16 04 2023].

Bermejo, B., Juiz, C. & Guerrero, c., 2019. Virtualization and consolidation: a systematic review of the past 10 years of research on energy and performance. *The journal of supercomputing,* 75(2), pp. 808-836.

Braden, A., 2021. *VMWare Workstation.* [Online] Available at: https://www.webopedia.com/definitions/vmware-workstation/
[Accessed 10 04 2023].

Chouffani, R., 2023. *IT asset management (ITAM).* [Online] Available at: https://www.techtarget.com/searchcio/definition/IT-asset-management-information-technology-asset-management
[Accessed 15 04 2023].

clearfind, 2023. *What is PDQ deploy?.* [Online] Available at: https://clearfind.com/guides/products/pdq-deploy
[Accessed 05 04 2023].

Collegenote, 2018. *Why an evolutionary prototyping is used in software development? Explain..* [Online]
Available at: https://www.collegenote.net/pastpapers/4420/question/
[Accessed 30 03 2023].

CyberHoot, 2020. *Demilitarized Zone (DMZ).* [Online] Available at: https://cyberhoot.com/cybrary/demilitarized-zone-dmz/
[Accessed 30 03 2023].

Debian.org, 2023. *Debian 11 bullseye.* [Online] Available at: https://www.debian.org/News/2021/20210814 [Accessed 10 04 2023].

Deshpande, C., 2022. *What Is Firewall: Types, How Does It Work, Advantages & Its Importance.* [Online] Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall [Accessed 15 04 2023].

Dudley, A., Braman , J., Wang, K. & Vincenti, G., 2023. *Security, Legal, and Ethical Implications of Using Virtual Worlds.* [Online] Available at: https://www.researchgate.net/publication/228968768_Security_Legal_and_Ethical_Implications_of_Using_Virtual_Worlds [Accessed 10 04 2023].

Everest Bank Limited, 2023. *Everest Bank Limited.* [Online] Available at: https://everestbankltd.com/ [Accessed 30 03 2023].

Feilz, F., 2022. *What is VMware ESXi?.* [Online] Available at: https://www.liquidweb.com/kb/what-is-vmware-esxi/ [Accessed 15 04 2023].

Fisher, T., 2021. *What Is a Router and How Does It Work?.* [Online] Available at: https://www.lifewire.com/what-is-a-router-2618162 [Accessed 15 04 2023].

Gantt Project, 2023. *Free desktop project management software.* [Online] Available at: https://www.ganttproject.biz/ [Accessed 10 04 2023].

GNS3, 2023. *Getting Started with GNS3.* [Online] Available at: https://docs.gns3.com/docs/#:~:text=GNS3%20is%20used%20by%20hundreds,even%20hosted

%20in%20the%20cloud.
[Accessed 10 04 2023].

gns3, 2023. *Which emulator should I use?.* [Online] Available at: https://docs.gns3.com/docs/emulators/which-emulators-should-i-use/ [Accessed 10 04 2023].

Gowda, T., Vanishree, S., MS, V. & K, Y., 2021. OVERVIEW OF VIRTUALIZATION IN CLOUD COMPUTING. *International Research Journal of Modernization in Engineering Technology and Science* , 03(07), pp. 1841-1846.

Grant, M., Khartit, K. & Kazel, M., 2022. *Gantt Charting: Definition, Benefits, and How They're Used.* [Online] Available at: https://www.investopedia.com/terms/g/gantt-chart.asp [Accessed 10 04 2023].

Hamilton, T., 2023. *Agile Methodology: What is Agile Model in Software Testing?.* [Online] Available at: https://www.guru99.com/agile-scrum-extreme-testing.html [Accessed 30 03 2023].

Kennedy, B., 2023. *Lansweeper pros and cons.* [Online] Available at: https://www.peerspot.com/products/lansweeper-pros-and-cons [Accessed 30 03 2023].

Leeron Hoory, C. B., 2022. *What Is Waterfall Methodology? Here's How It Can Help Your Project Management Strategy.* [Online] Available at: https://www.forbes.com/advisor/business/what-is-waterfall-methodology/ [Accessed 16 03 2023].

Martinez, P., 2023. *What is Evolutionary Prototype?.* [Online] Available at: https://mockitt.wondershare.com/prototyping/evolutionary-prototyping.html [Accessed 30 03 2023].

Mohanan, R., 2022. *DevOps vs. Agile Methodology: Key Differences and Similarities.* [Online] Available at: https://www.spiceworks.com/tech/devops/articles/devops-vs-agile/ [Accessed 30 03 2023].

Nepal News, 2023. *8 arrested for hacking bank accounts using mobile apps.* [Online] Available at: https://nepalnews.com/s/capital/8-arrested-for-hacking-bank-accounts-using-mobile-apps
[Accessed 30 03 2023].

Patel, M., 2020. *Demilitariz Demilitarized Zone: An Ex one: An Exceptional La ceptional Layer of Network Security t er of Network Security to.* [Online] Available at: https://scholar.uwindsor.ca/cgi/viewcontent.cgi?article=9311&context=etd
[Accessed 15 03 2023].

Powell, R., 2022. *Advantages and Disadvantages of Virtualization.* [Online] Available at: https://circleci.com/blog/top-6-benefits-of-virtualization/
[Accessed 10 04 2023].

Prasain, K., 2022. *The Kathmandu Post.* [Online] Available at: https://kathmandupost.com/money/2022/12/21/nepal-ranks-way-down-in-digital-entrepreneurship-and-innovation
[Accessed 30 03 2023].

Pratik Ragnarson, N. G., 2018. *Firewall implementation and testing.* [Online] Available at: https://www.ida.liu.se/~TDDD17/oldprojects/2009/projects/012-2.pdf
[Accessed 15 03 2023].

Rouse, M., 2020. *What Does Microsoft Office Mean?.* [Online] Available at: https://www.techopedia.com/definition/20737/microsoft-office
[Accessed 15 04 2023].

Sharma, R. D., 2017. *Nepali banks 'not prepared' to ward off cyber threats.* [Online] Available at: https://kathmandupost.com/money/2017/10/25/nepali-banks-not-prepared-to-ward-off-cyber-threats
[Accessed 30 03 2023].

Shrimali, S., 2017. DeMilitarized Zone: Network Architecture for Information Security. *International Journal of Computer Applications (0975 – 8887),* 174(5), pp. 16-19.

Singh, A., 2022. *What Is A Network Switch And Its Types.* [Online] Available at: https://www.shiksha.com/online-courses/articles/network-switch-and-its-types/ [Accessed 15 04 2023].

UKessays, 2019. *Waterfall Methodology in Software Development.* [Online] Available at: https://www.ukessays.com/essays/computer-science/waterfall-methodology-in-software-development.php
[Accessed 30 03 2023].

Westland, J., 2022. *Scrum Methodology: Roles, Events & Artifacts.* [Online] Available at: https://www.projectmanager.com/blog/scrum-methodology [Accessed 30 03 2023].

Willlians, E., 2022. *How to Deploy Software with PDQ Deploy - Updated.* [Online] Available at: https://pdf.wondershare.com/business/how-to-deploy-software-with-pdq-deploy.html
[Accessed 15 04 2023].

Zaharia, A., 2023. *300+ Terrifying Cybercrime and Cybersecurity Statistics (2023 EDITION).* [Online]
Available at: https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
[Accessed 30 03 2023].

Zavadsky, V., 2022. *DMZ Network: How It Works, Its Uses, and Benefits in Network Security.* [Online]
Available at: https://www.linkedin.com/pulse/dmz-network-how-works-its-uses-benefits-security-valdemar-z%C3%A1vadsk%C3%BD
[Accessed 13 04 2023].

CHAPTER 8: APPENDIX

8.1. Appendix A: Pre-Survey Results

8.1.1. Presurvey form

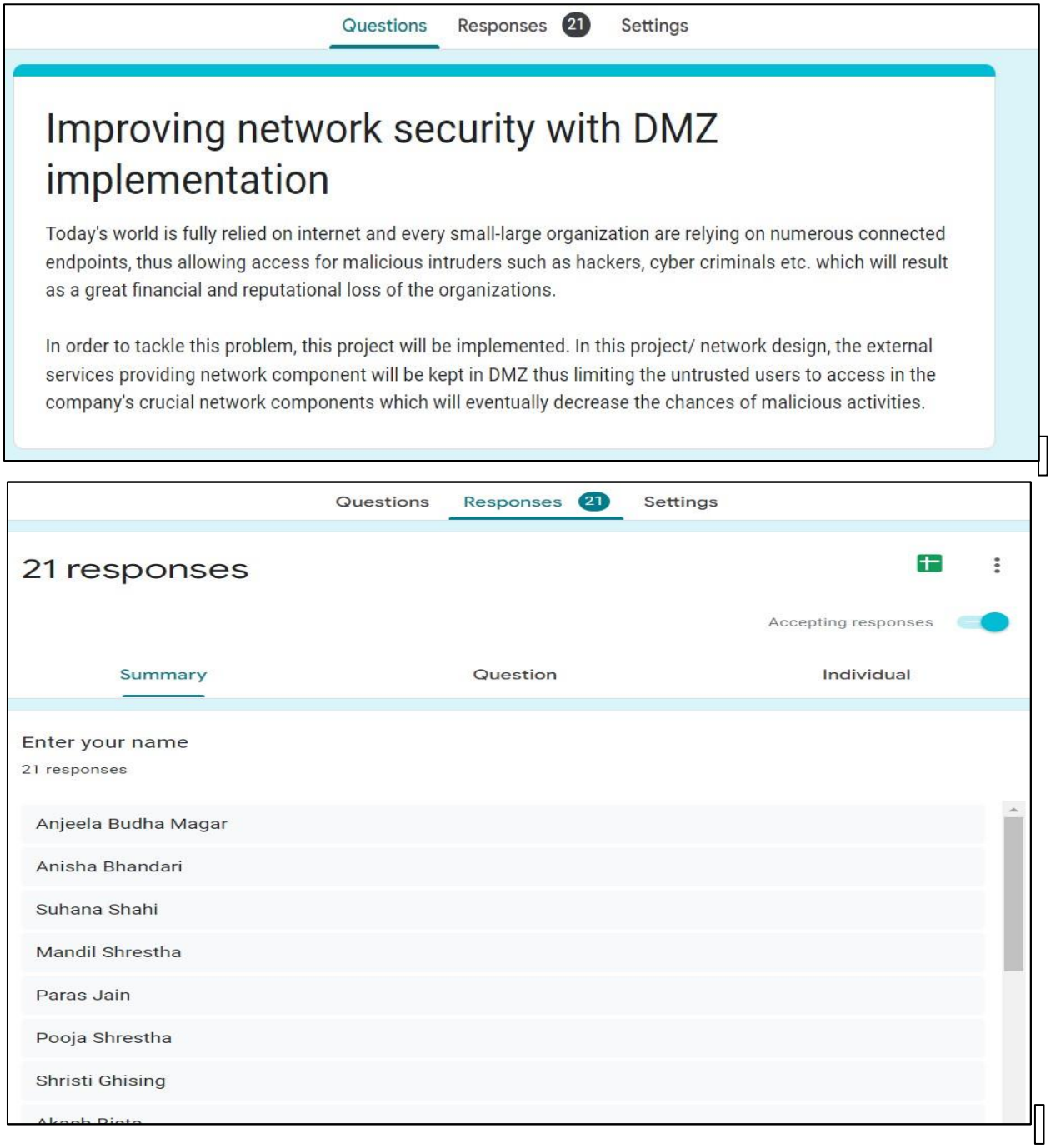


Figure 102 Presurvey form

8.1.2. Sample of filled pre-survey form.

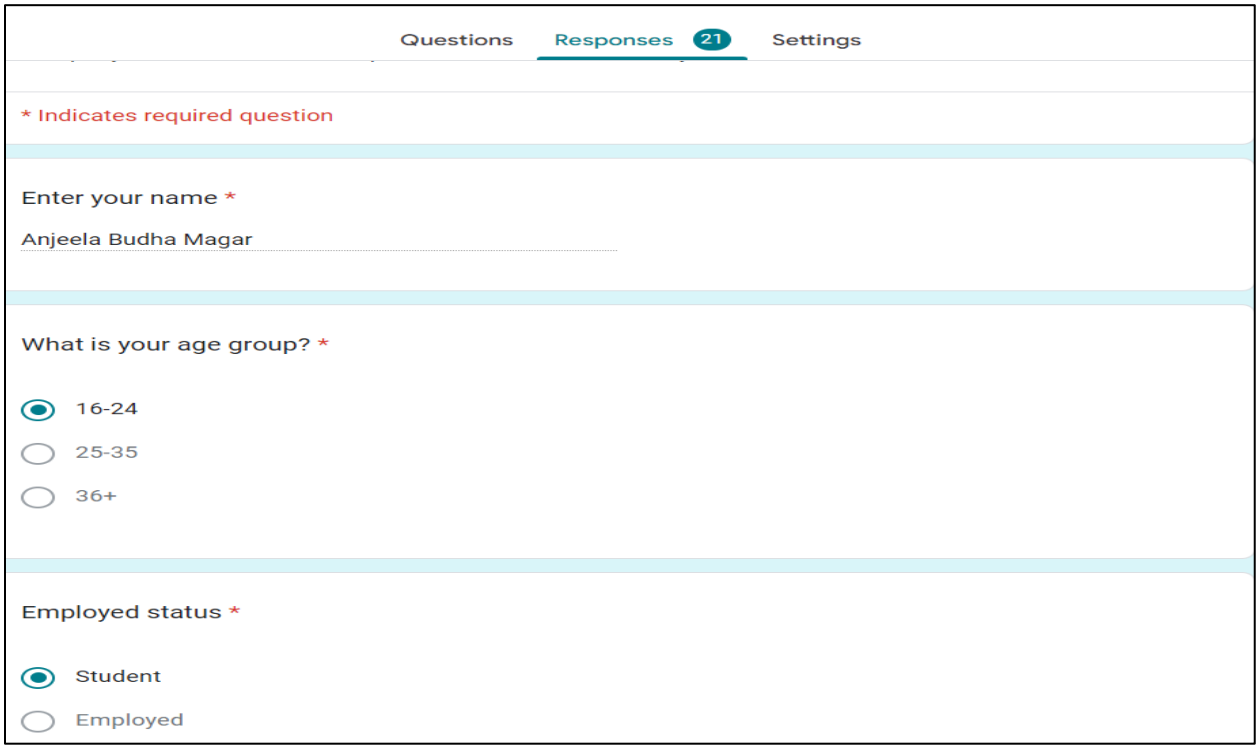


Figure 103 Sample of pre-survey form (1)

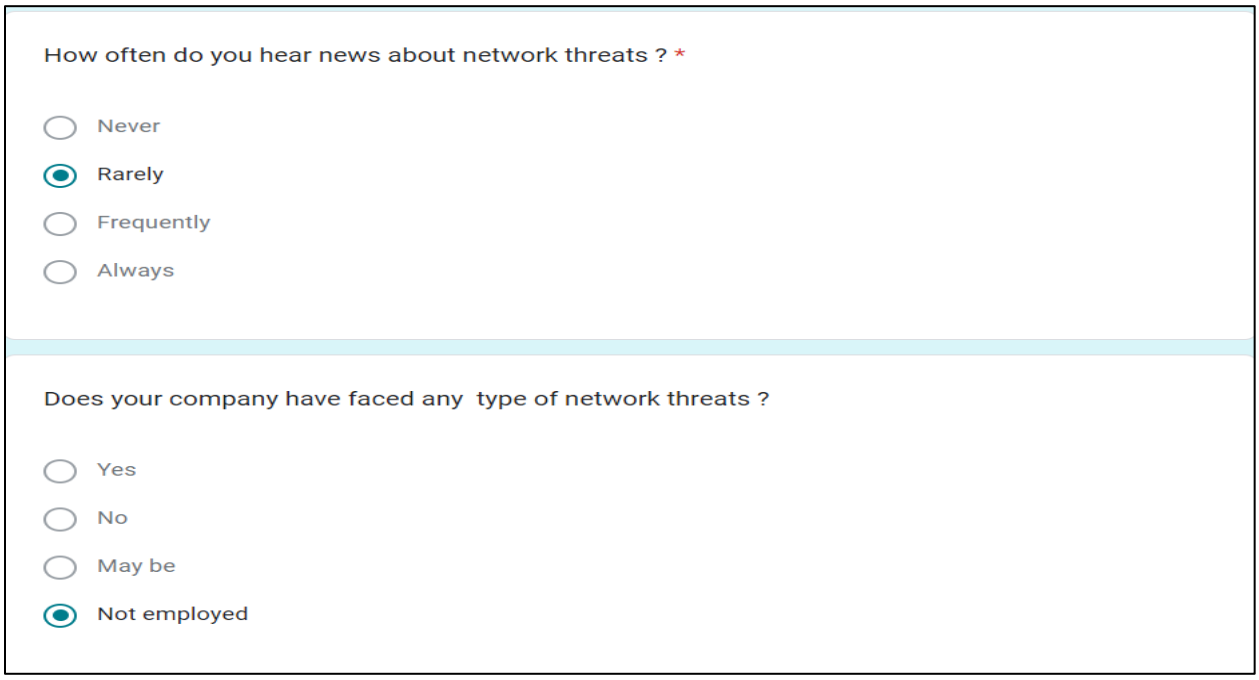


Figure 104 Sample of pre-survey form (2)

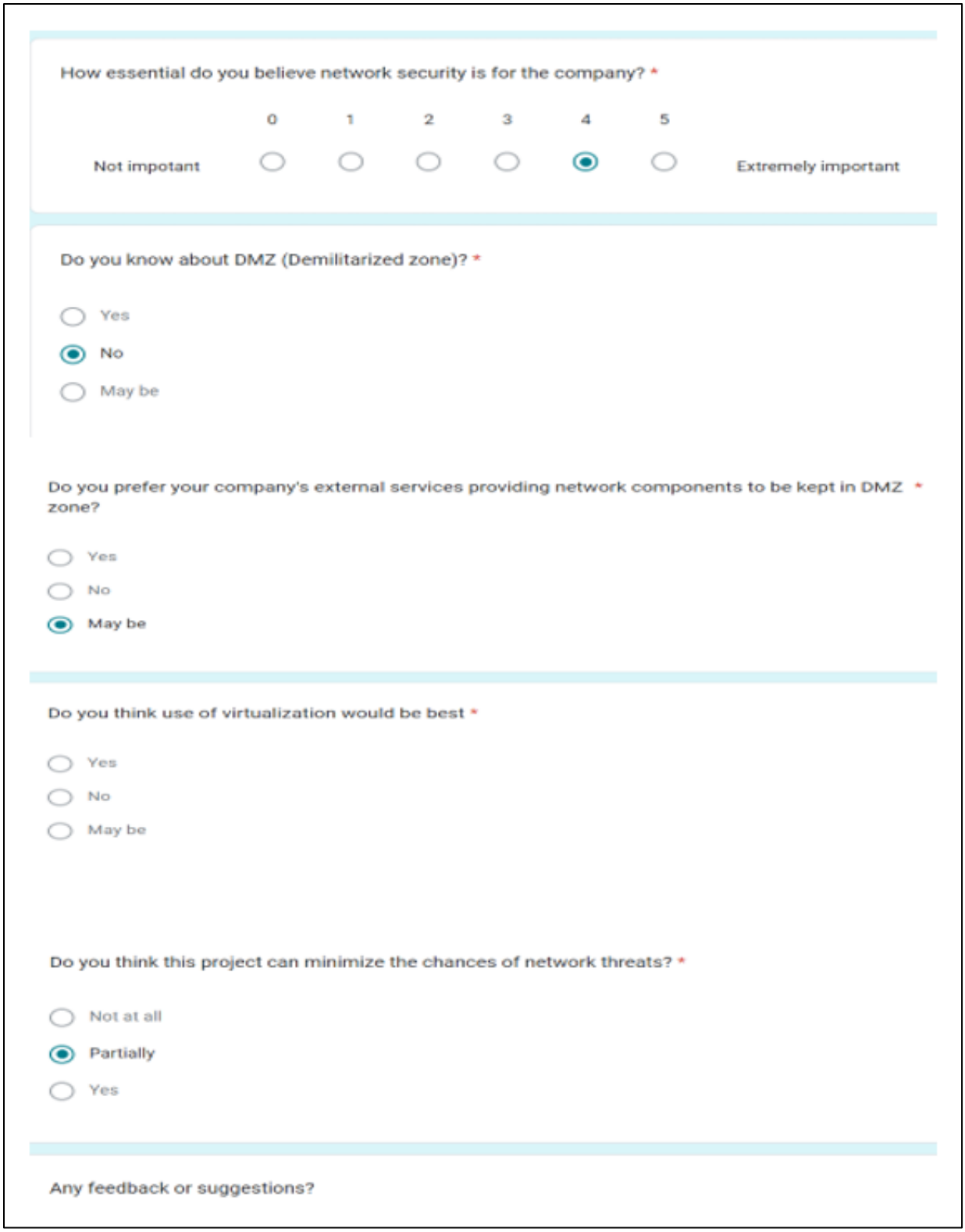


Figure 105 Sample of pre survey form (3)

8.1.3. Pre-survey results

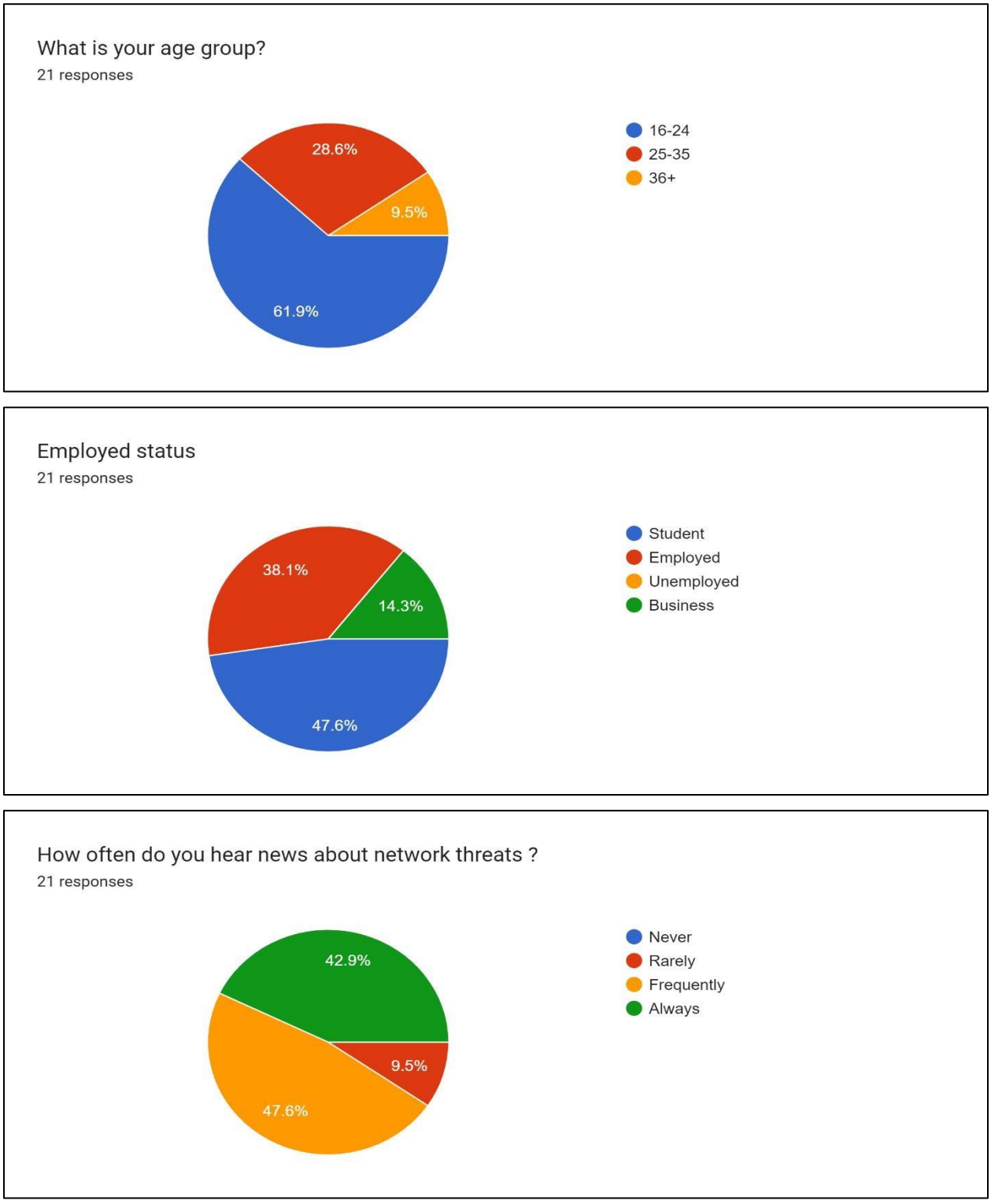


Figure 106 Pre-survey results (1)

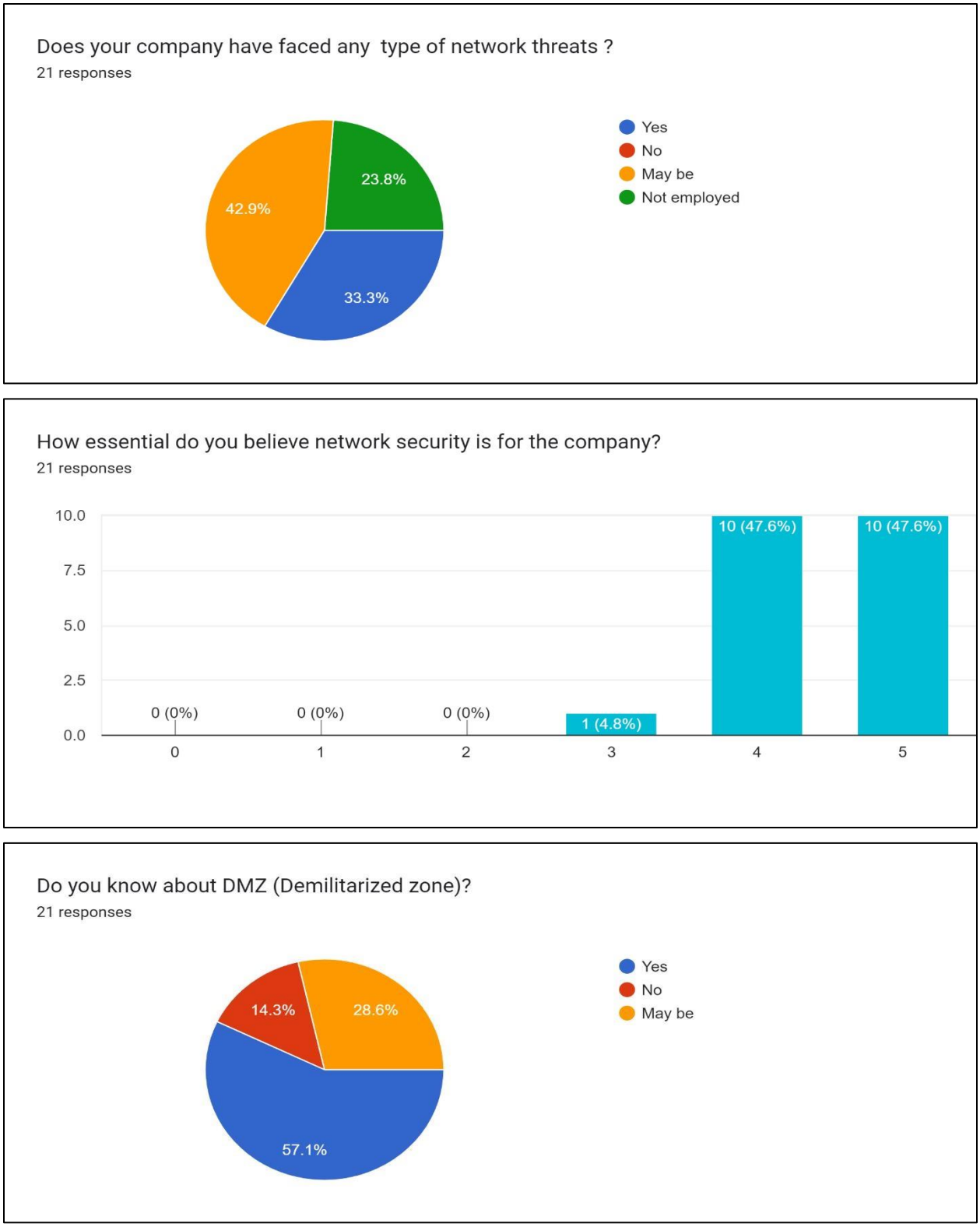


Figure 107 Pre-survey results (2)

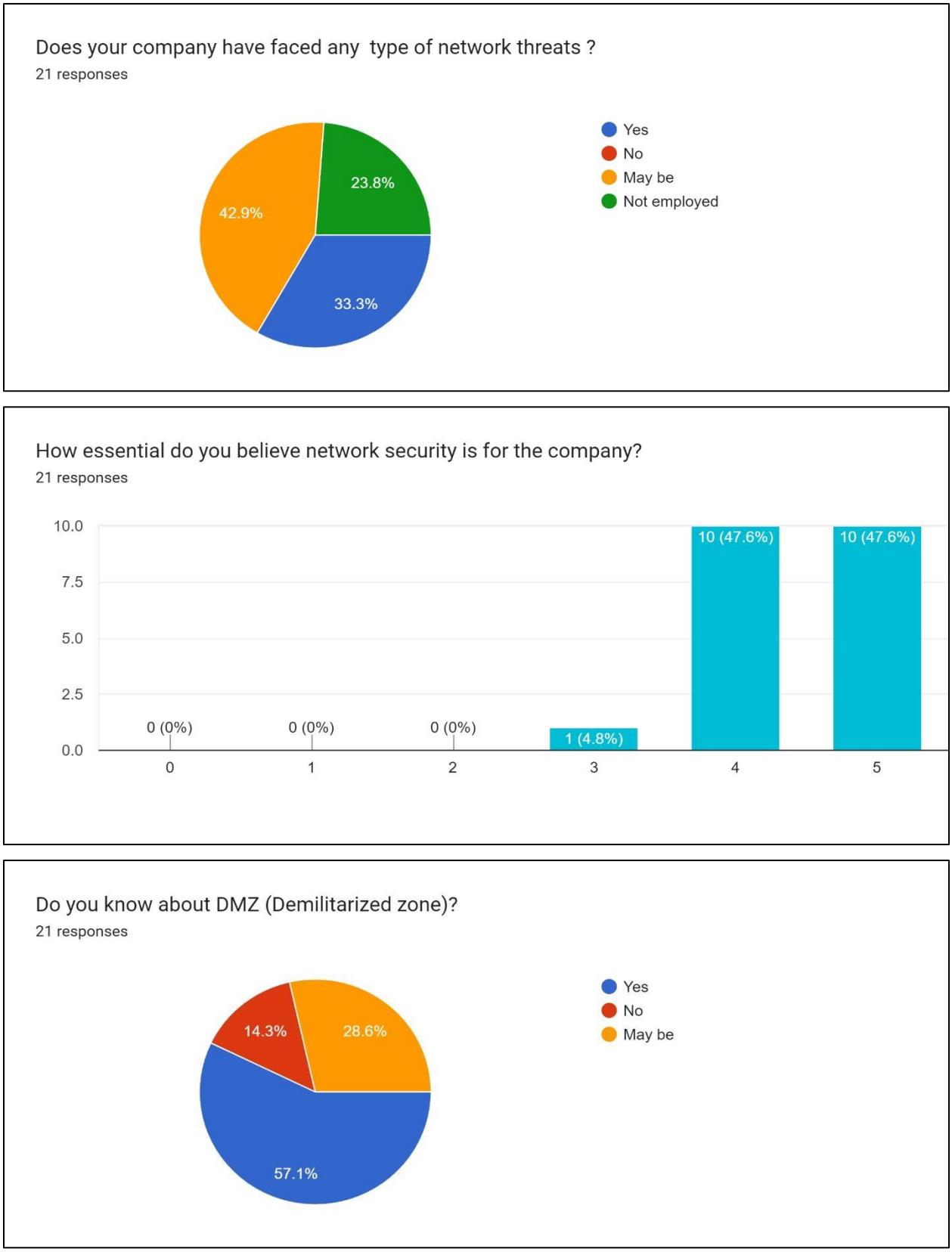


Figure 108 Pre-survey results (3)

8.2. Appendix B: Post Survey Results

8.2.1. Post-survey form

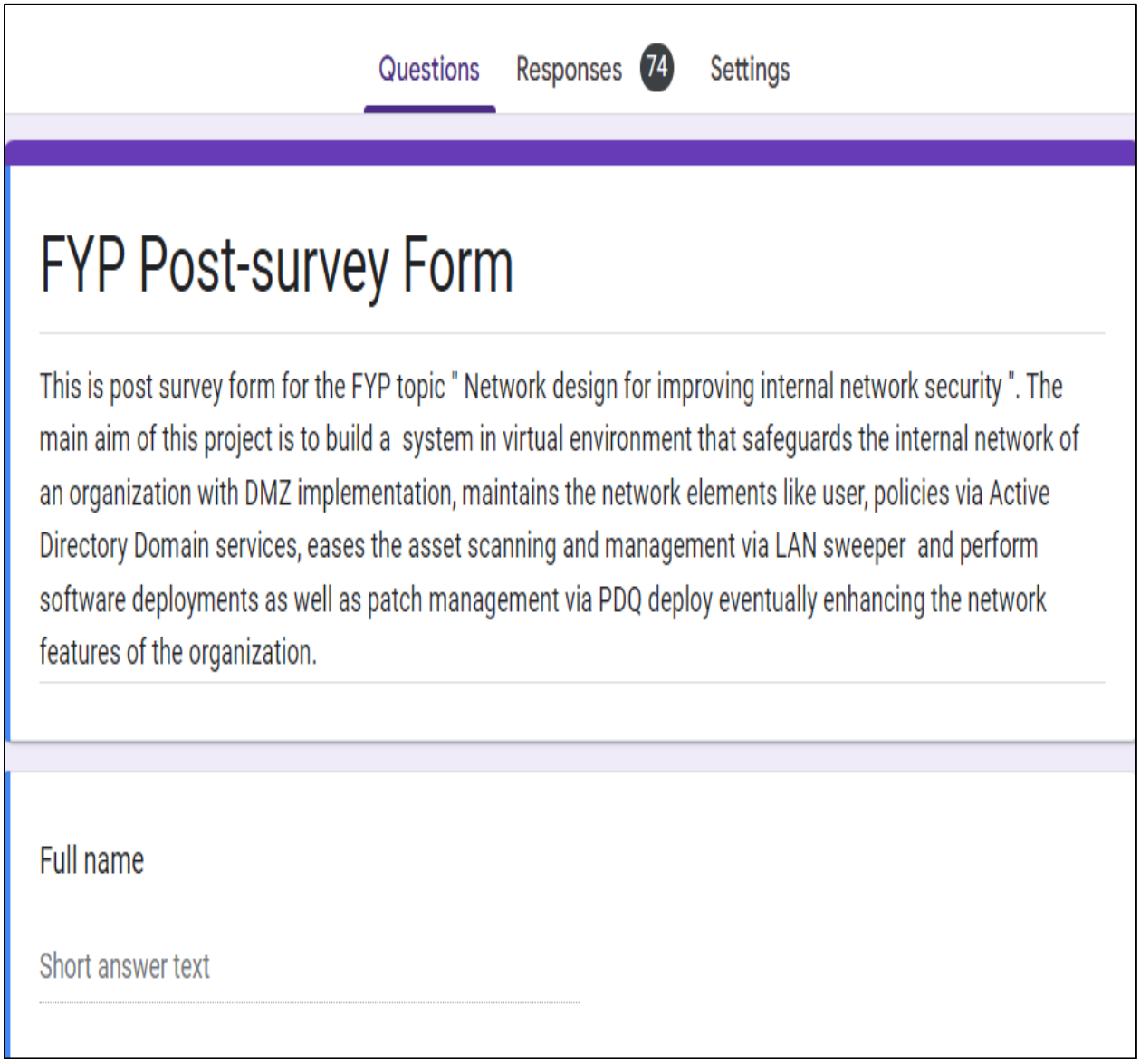


Figure 109 post-survey form.

8.2.2. Sample of the filled post-survey form.

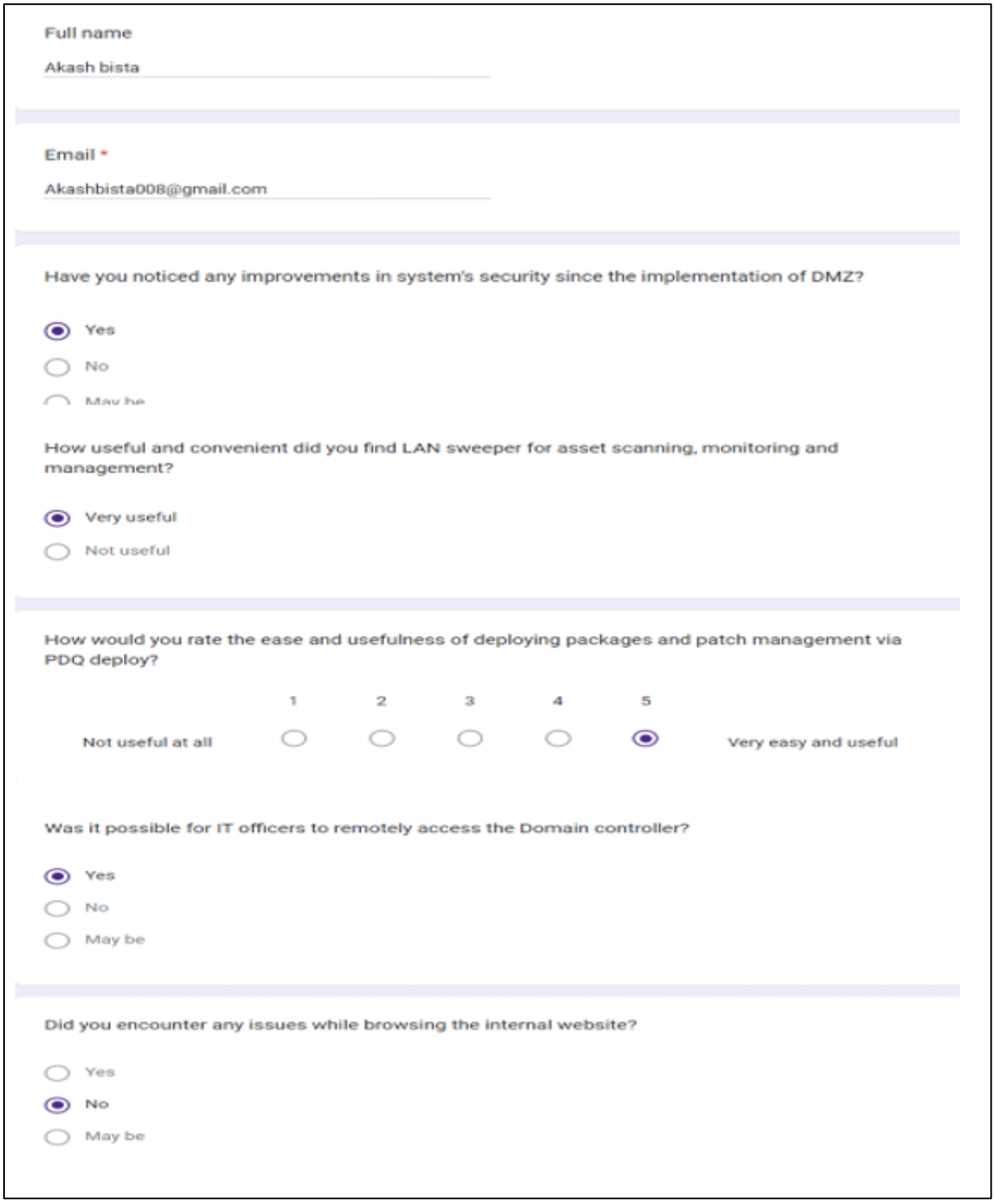


Figure 110 Sample of the filled post-survey form (1.)

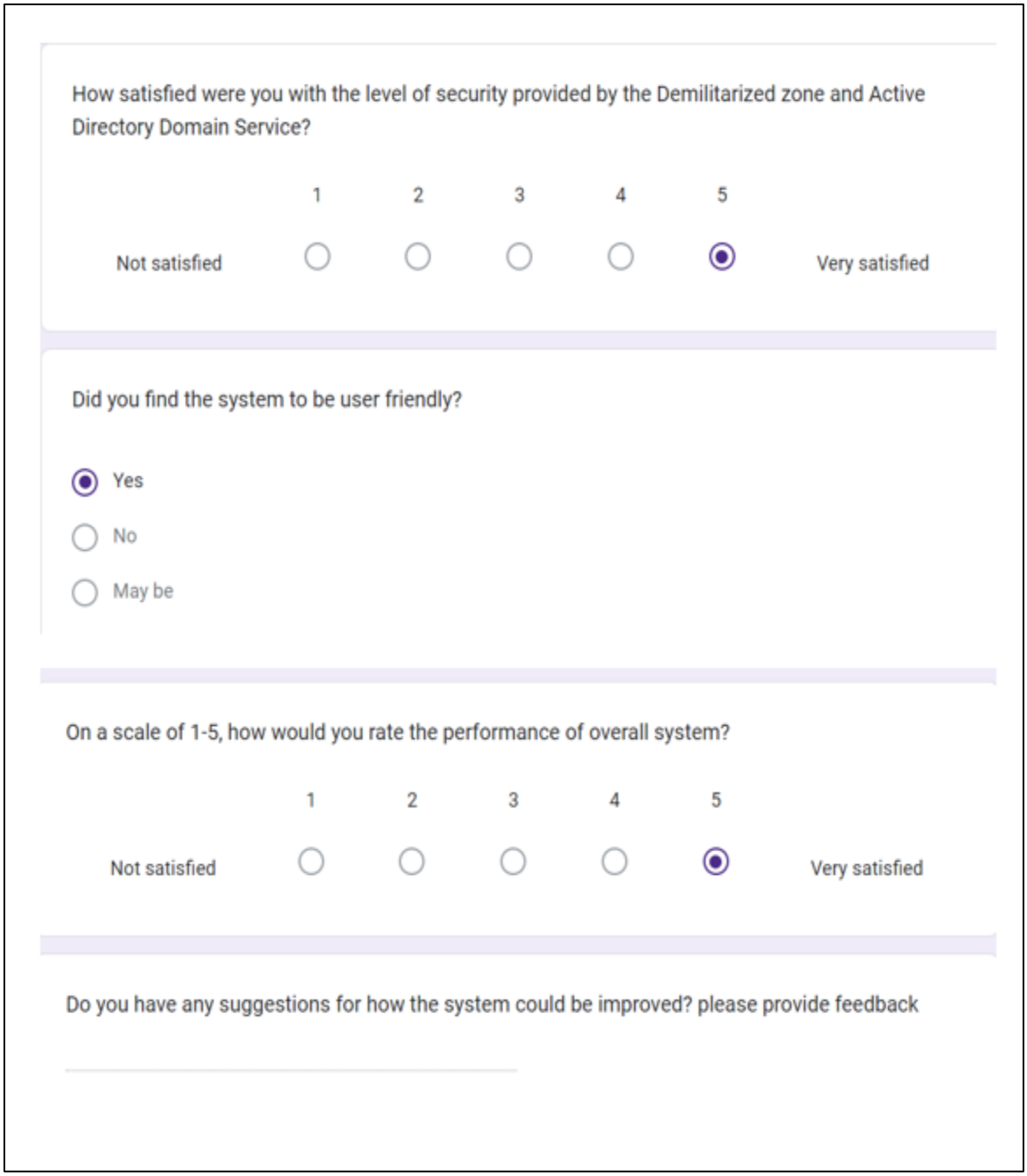


Figure 111 Sample of the filled post-survey form (2).

8.2.3. Post-survey result

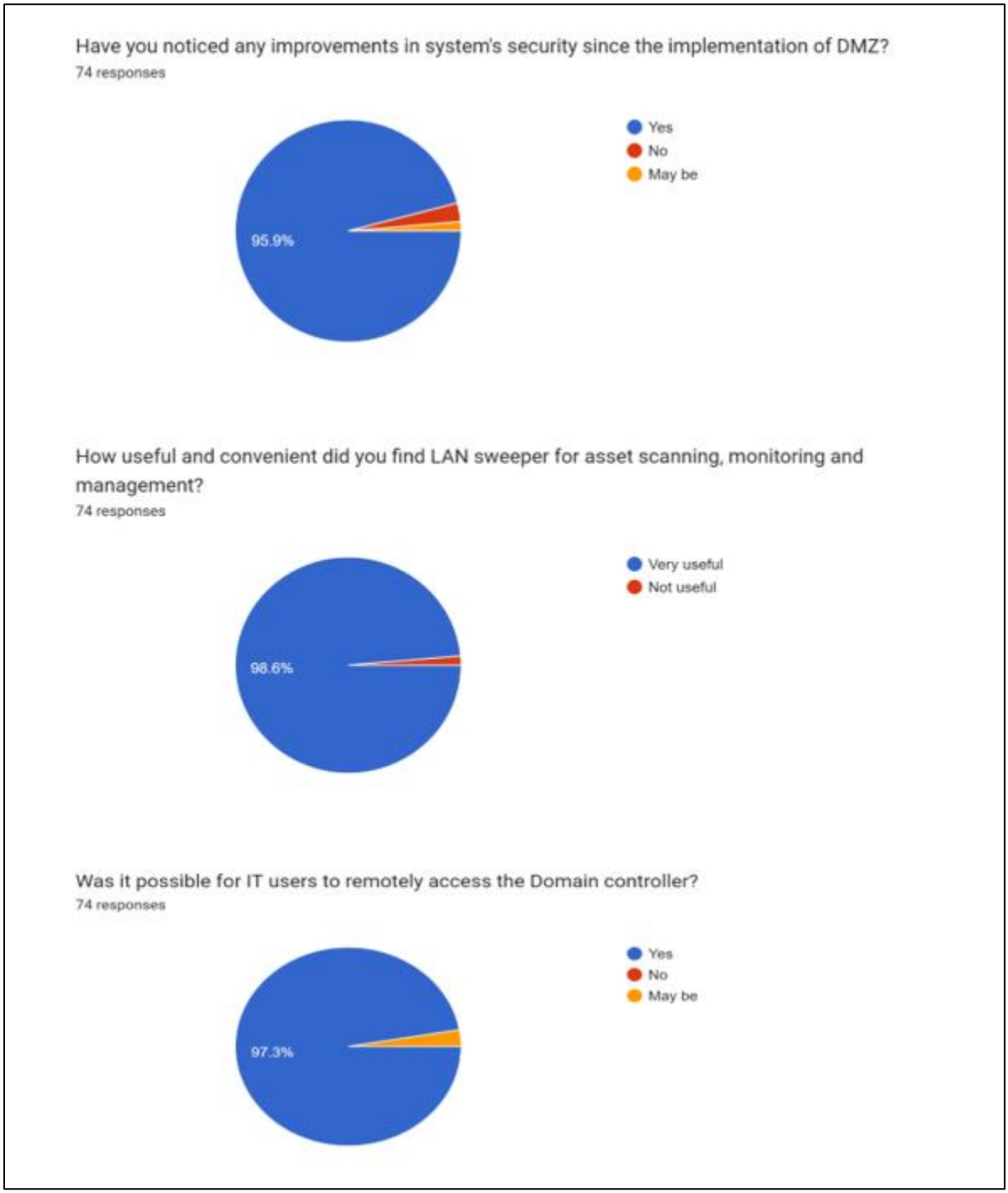


Figure 112 post-survey results (1).

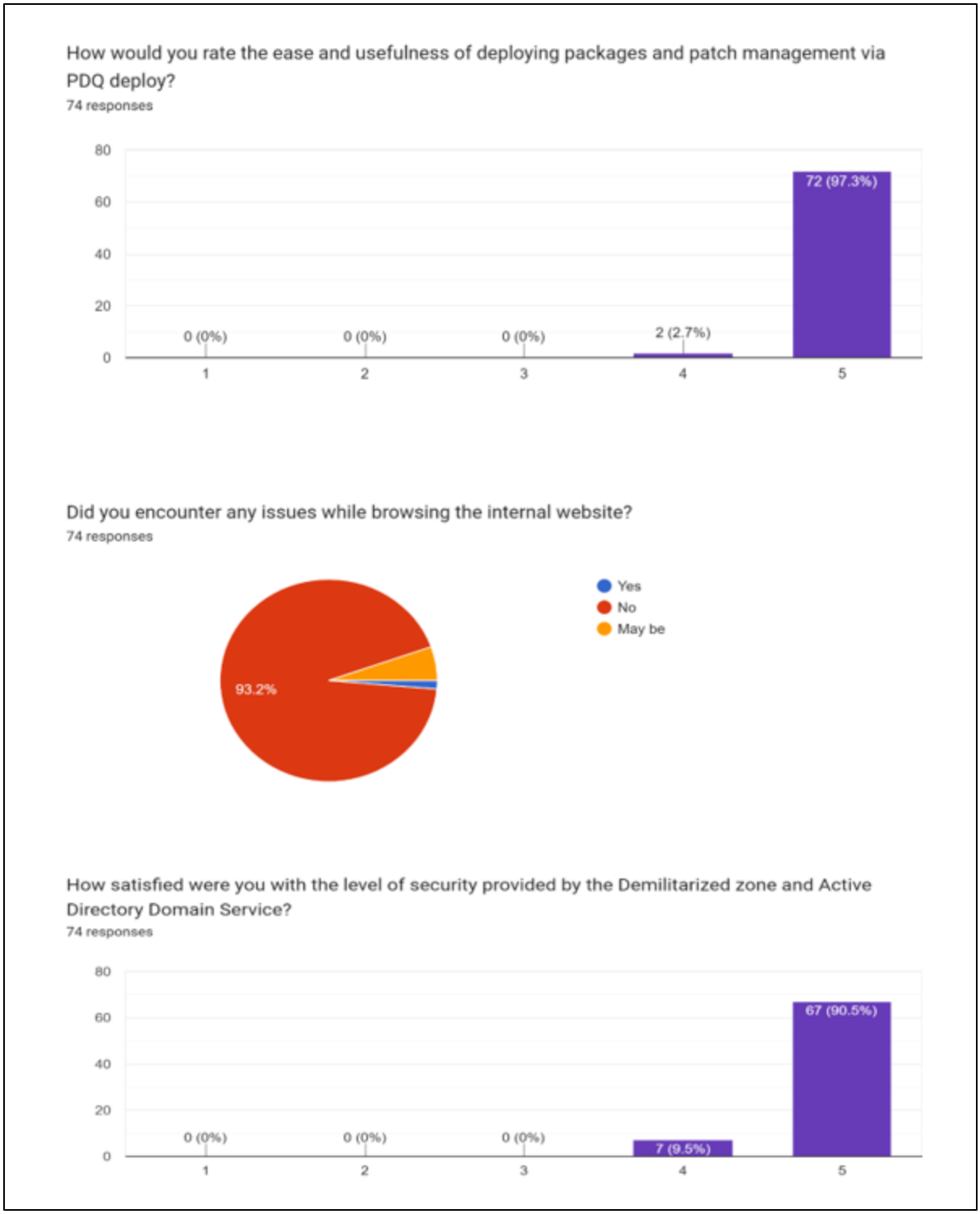


Figure 113 post-survey results (2).

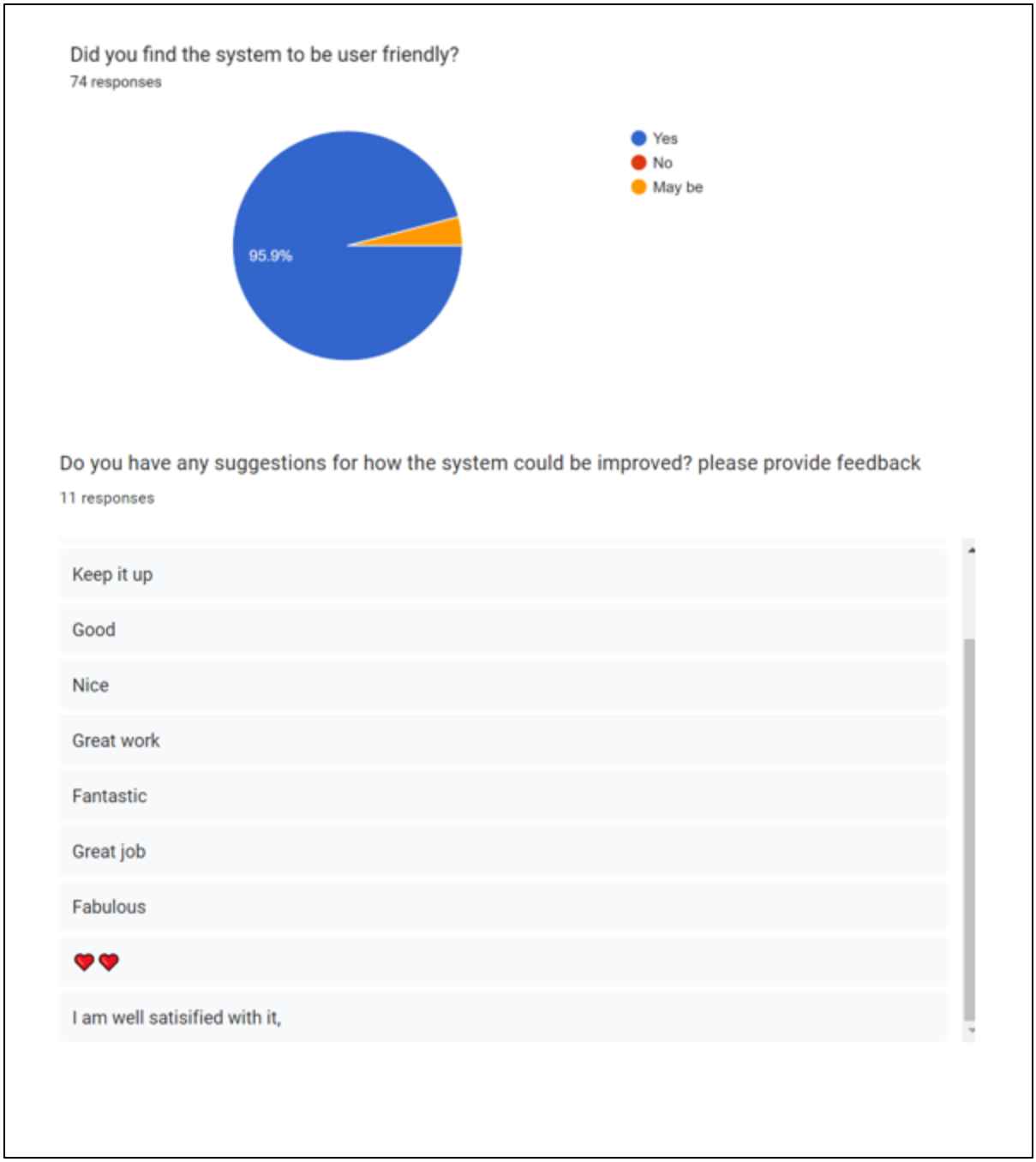


Figure 114 post-survey results (3).

8.3. Appendix C: Initial developed system's screenshot

8.3.1. gns3 and gns3 VM configuration.

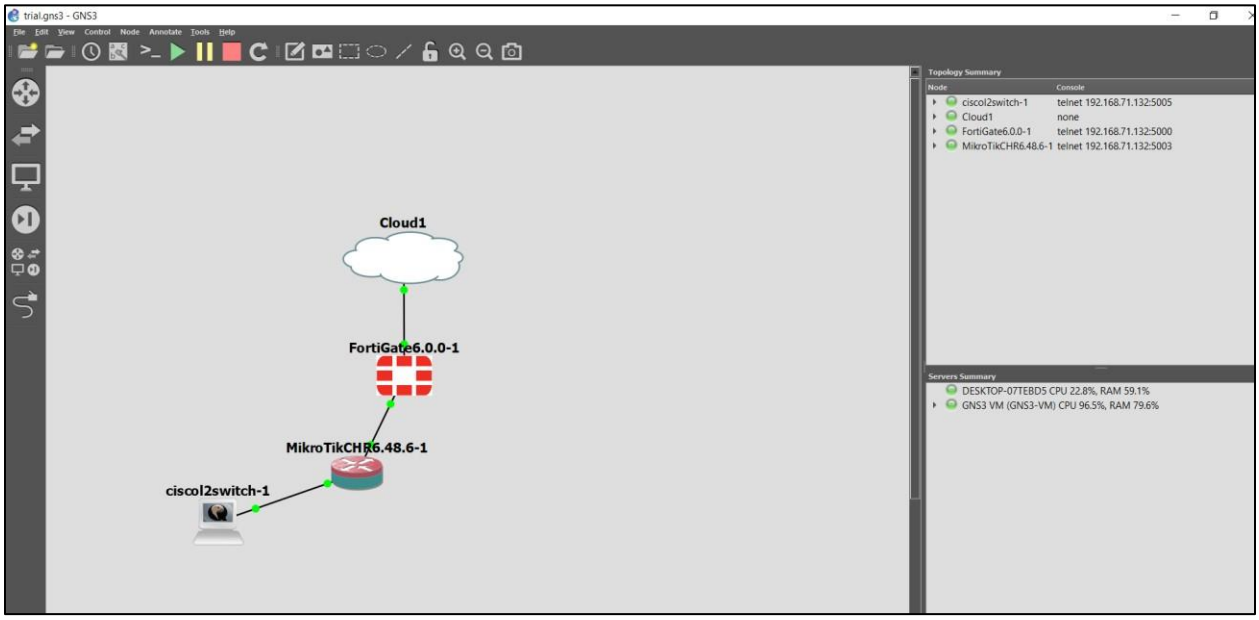


Figure 115 gns3 interface

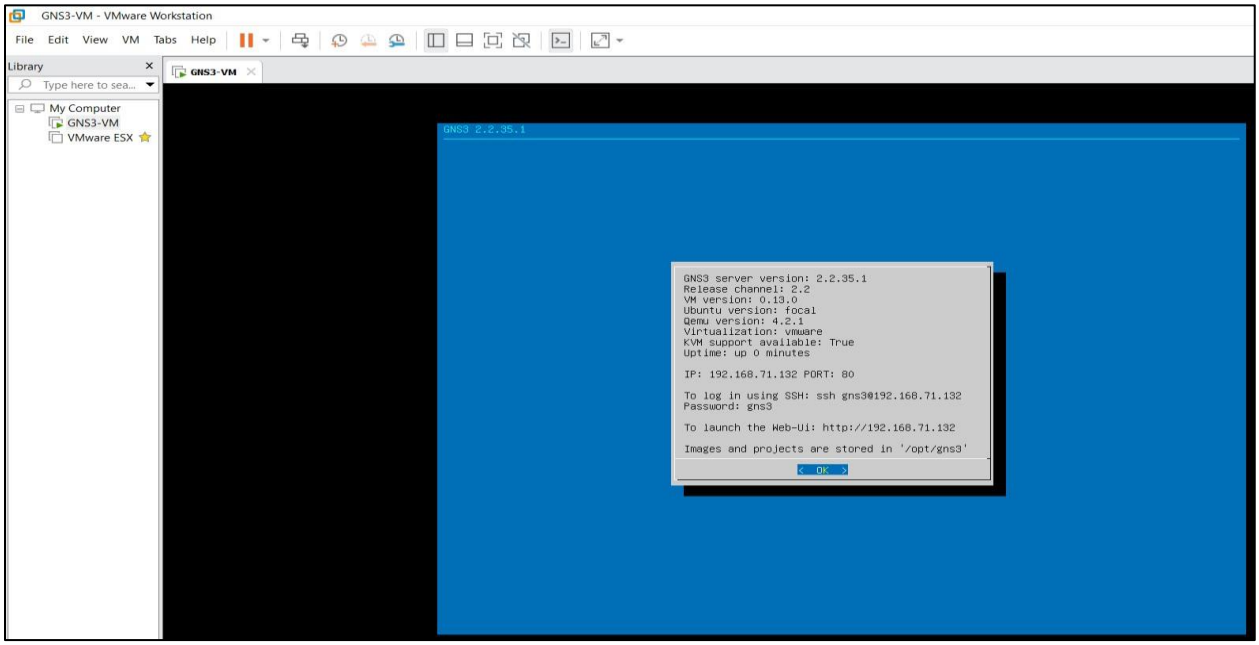


Figure 116 gns3 VM server interface

8.3.2. Firewall configuration

```
System is starting...
Starting system maintenance...
Scanning /dev/vda1... (100%)
Scanning /dev/vda2... (100%)
Serial number is FGVMEVLPRBIQQU4D


FortiGate-VM64-KVM login: admin
Password:
Welcome !

WARNING: File System Check Recommended! Unsafe reboot may have caused inconsiste
ncy in disk drive.
It is strongly recommended that you check file system consistency before proceed
ing.
Please run 'execute disk scan 17'
Note: The device will reboot and scan during startup. This may take up to an hou
r.
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port1

FortiGate-VM64-KVM (port1) # set mode static

FortiGate-VM64-KVM (port1) # set ip 192.168.71.4/24

FortiGate-VM64-KVM (port1) # set allowaccess ping http https telnet ssh

FortiGate-VM64-KVM (port1) # set role wan

FortiGate-VM64-KVM (port1) # set alias wan

FortiGate-VM64-KVM (port1) # end

FortiGate-VM64-KVM # execute ping 192.168.71.2
PING 192.168.71.2 (192.168.71.2): 56 data bytes
64 bytes from 192.168.71.2: icmp_seq=0 ttl=128 time=1.1 ms
64 bytes from 192.168.71.2: icmp_seq=1 ttl=128 time=0.8 ms
^C
--- 192.168.71.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.8/0.9/1.1 ms

FortiGate-VM64-KVM #
```

Figure 117 Firewall CLI interface

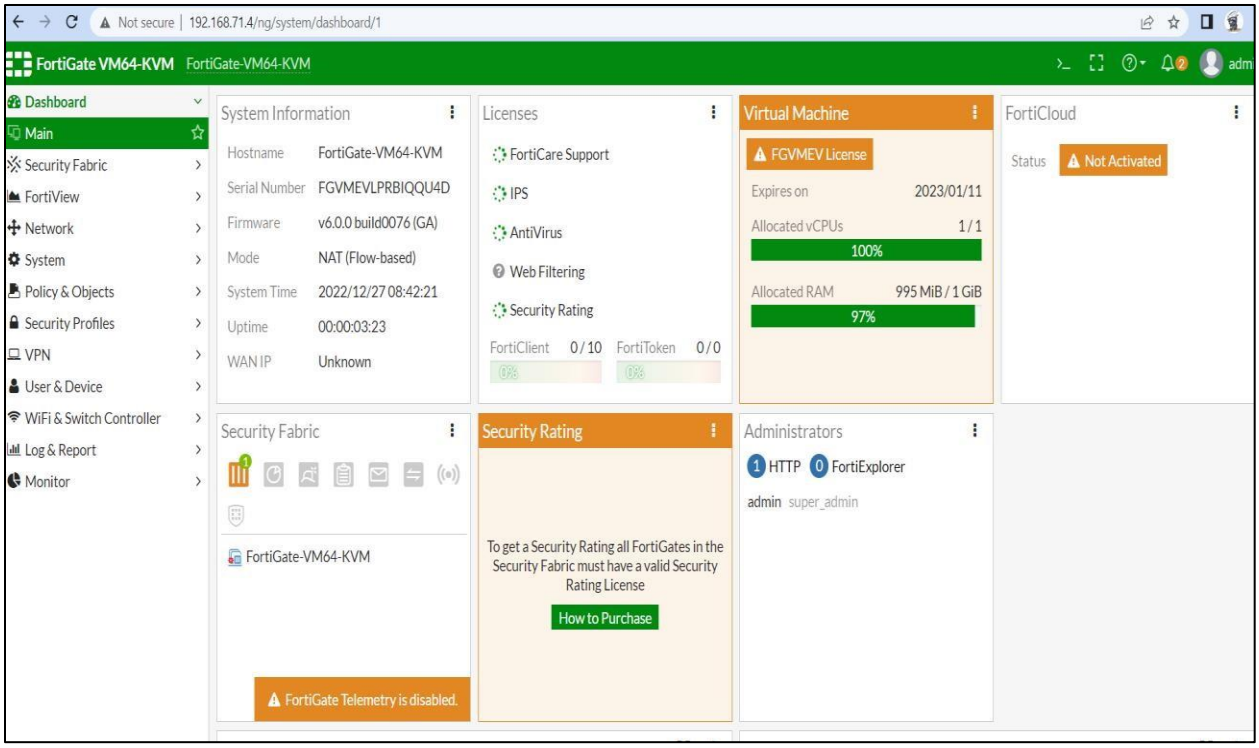


Figure 118 Firewall GUI interface

8.3.3. VMware ESXi configuration

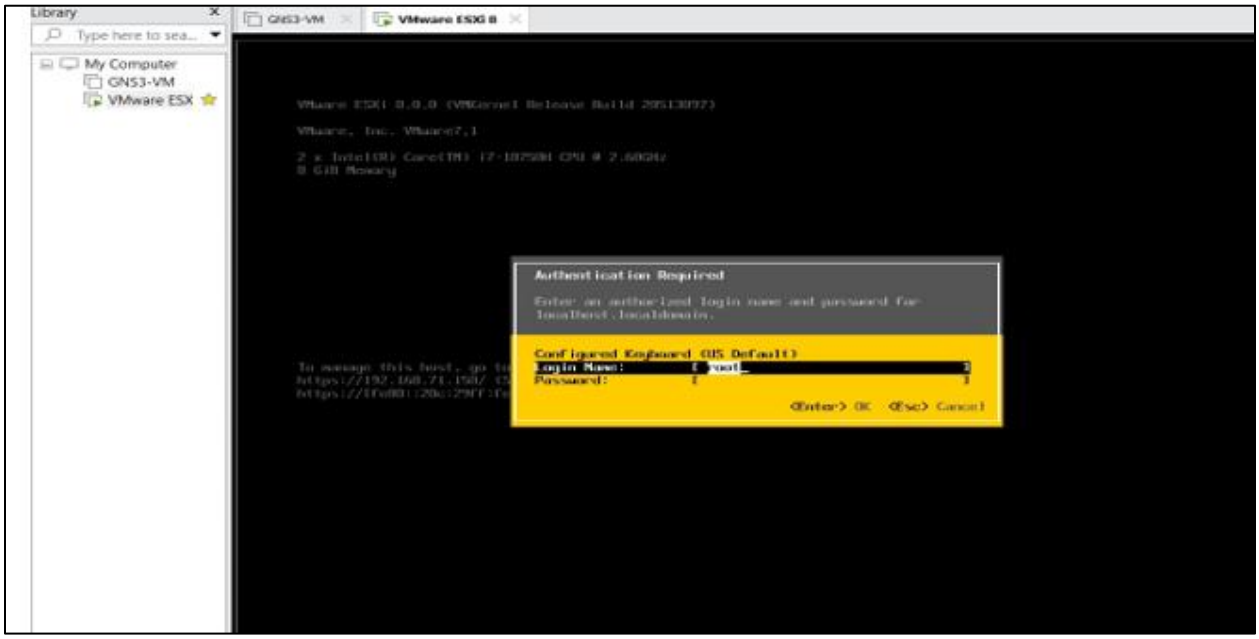


Figure 119 VMware ESXi console interface

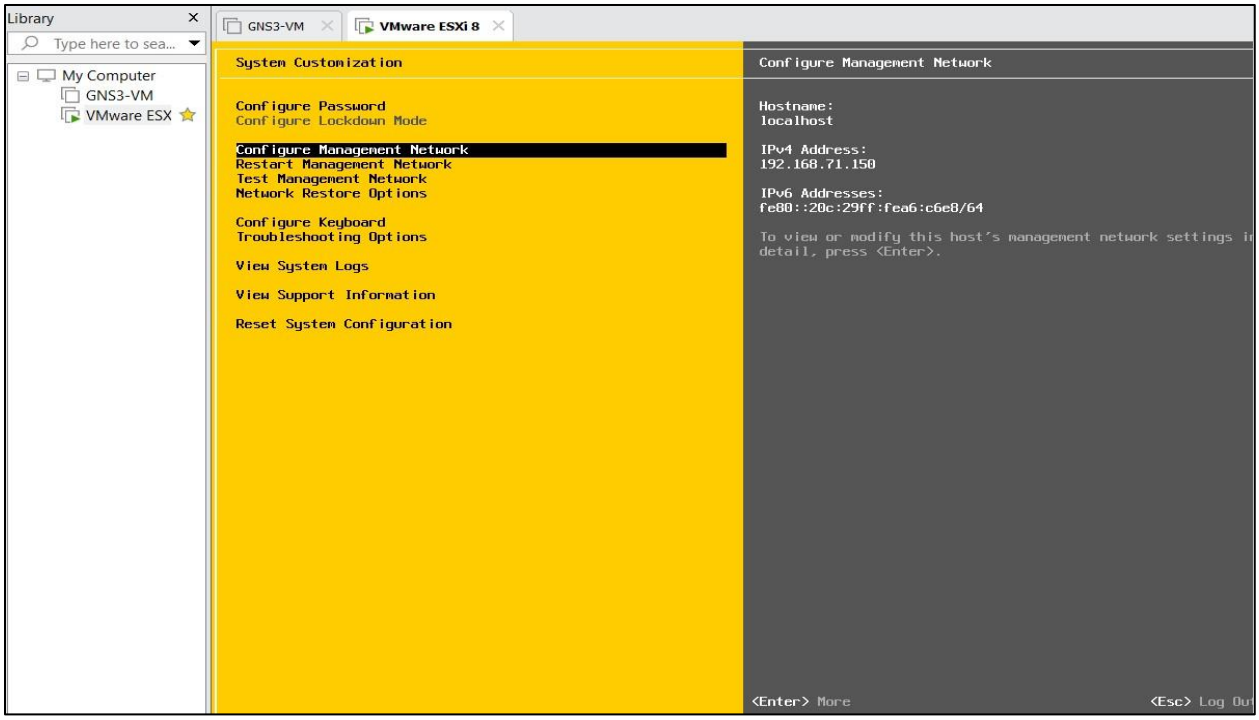


Figure 120 Static IP configuration

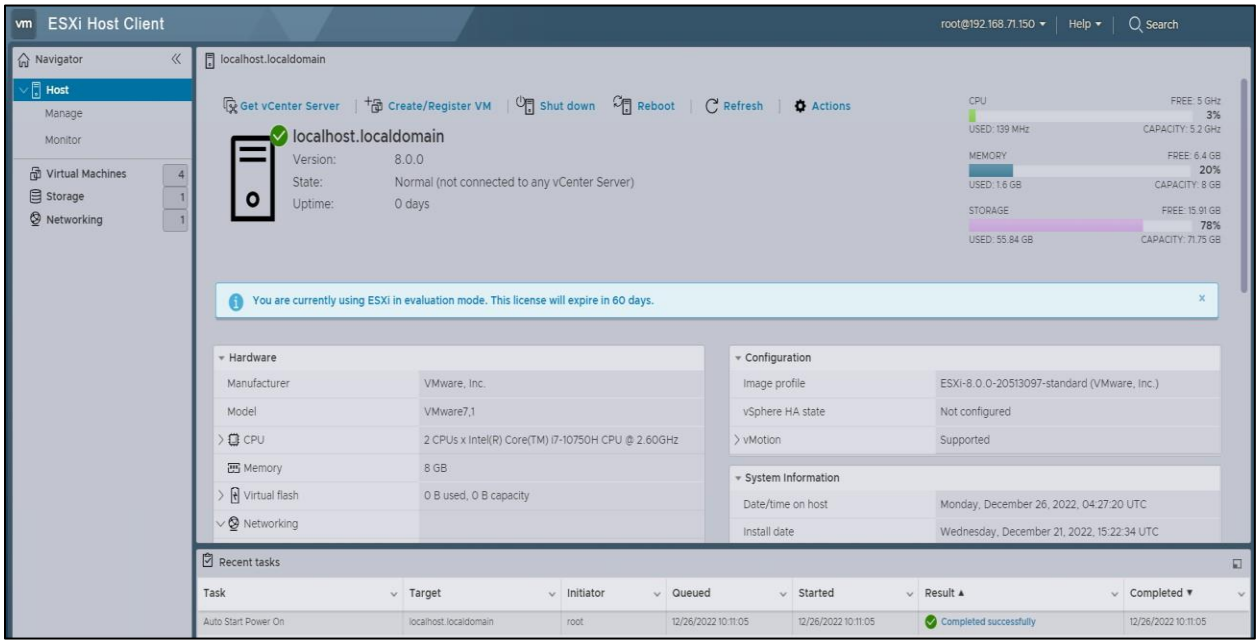


Figure 121 VMware ESXi GUI

8.3.4. Domain controller installation

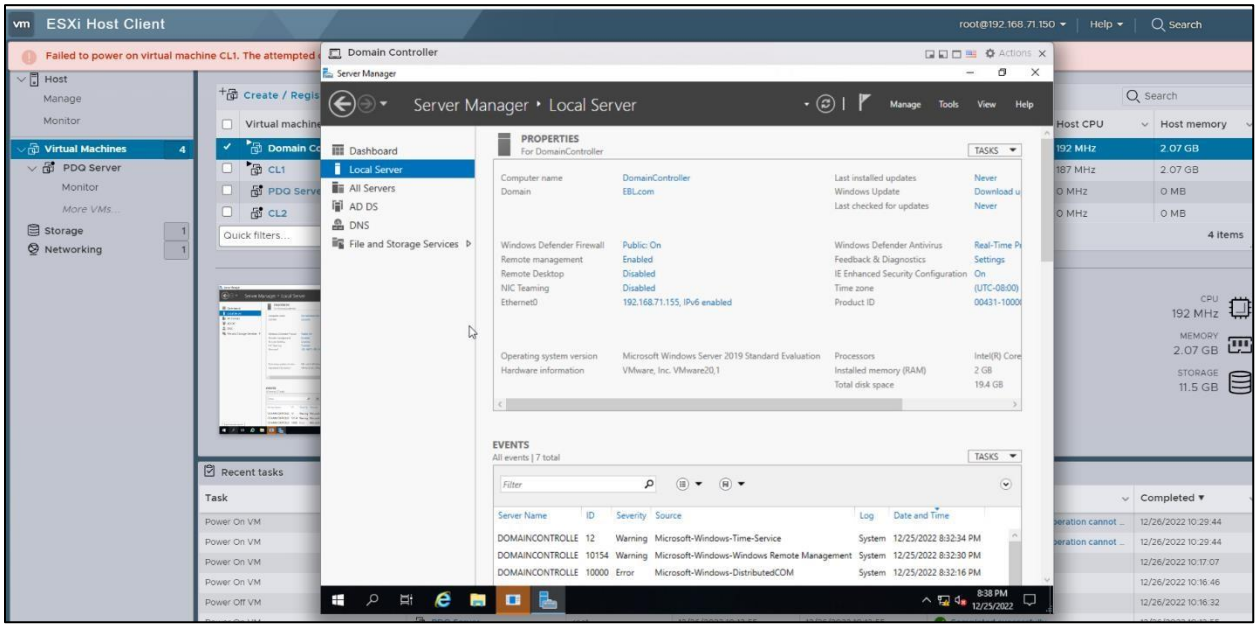


Figure 122 Domain controller

8.3.5. Clients Installation

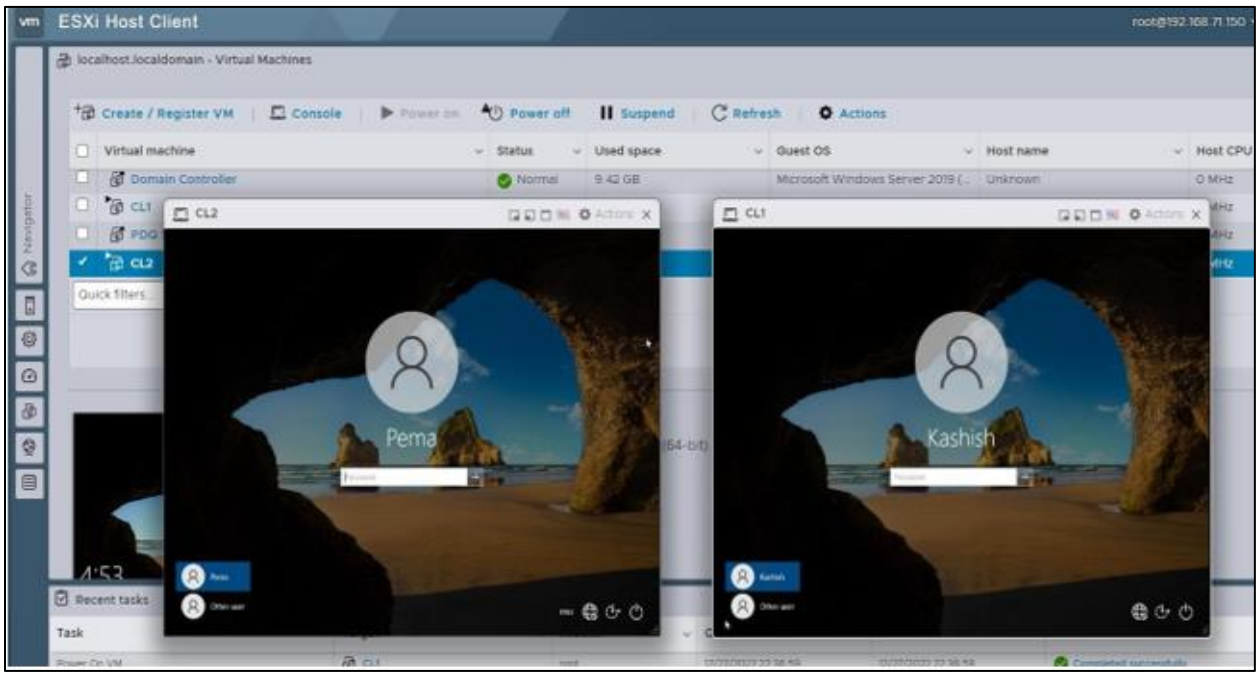


Figure 123 Clients under EBL.com

8.3.6. Web server installation.

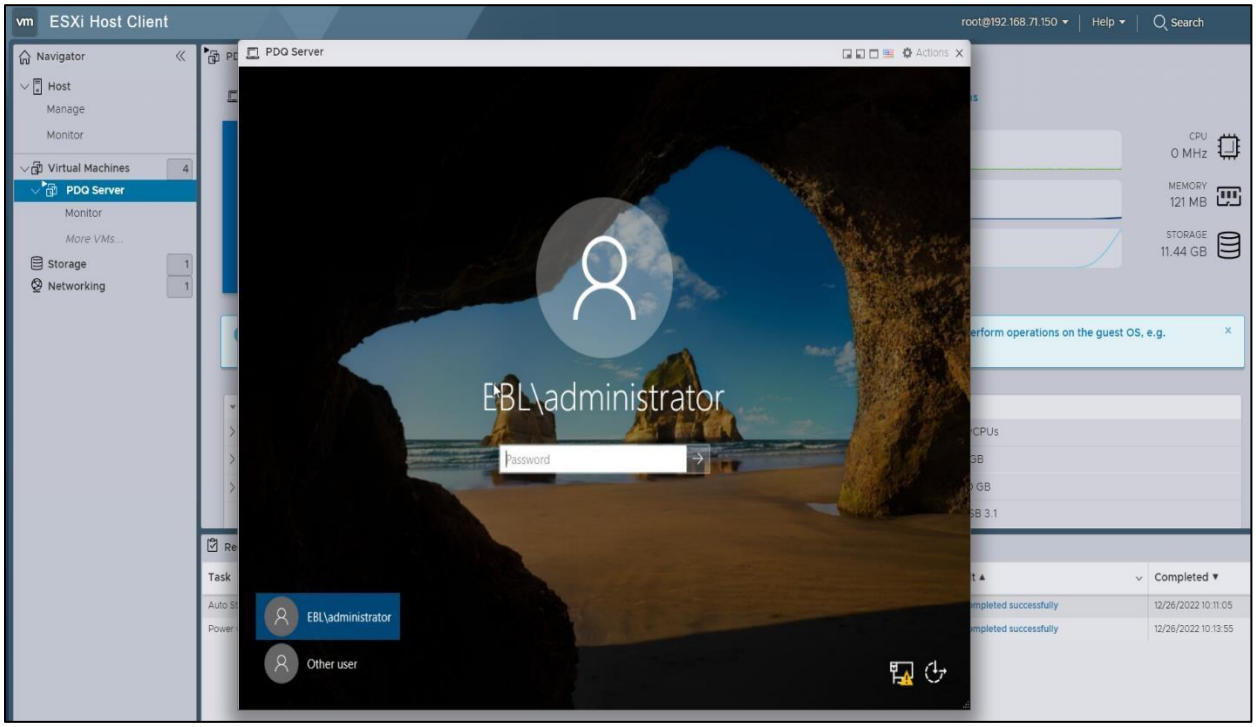


Figure 124 Internal web server

8.4. Appendix D: Final system's screenshots

8.4.1. FortiGate configuration

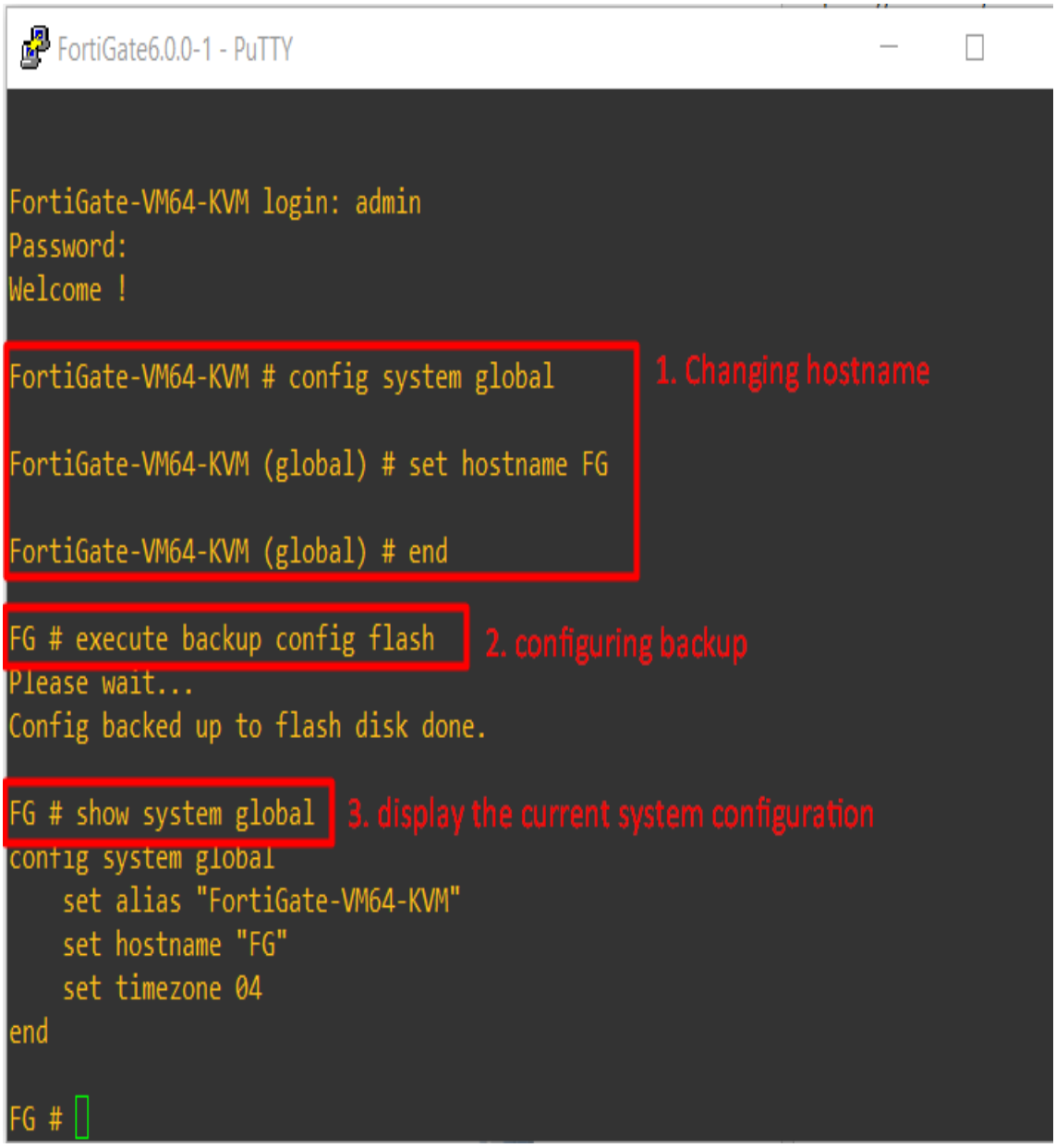


Figure 125 Changing host name of firewall.

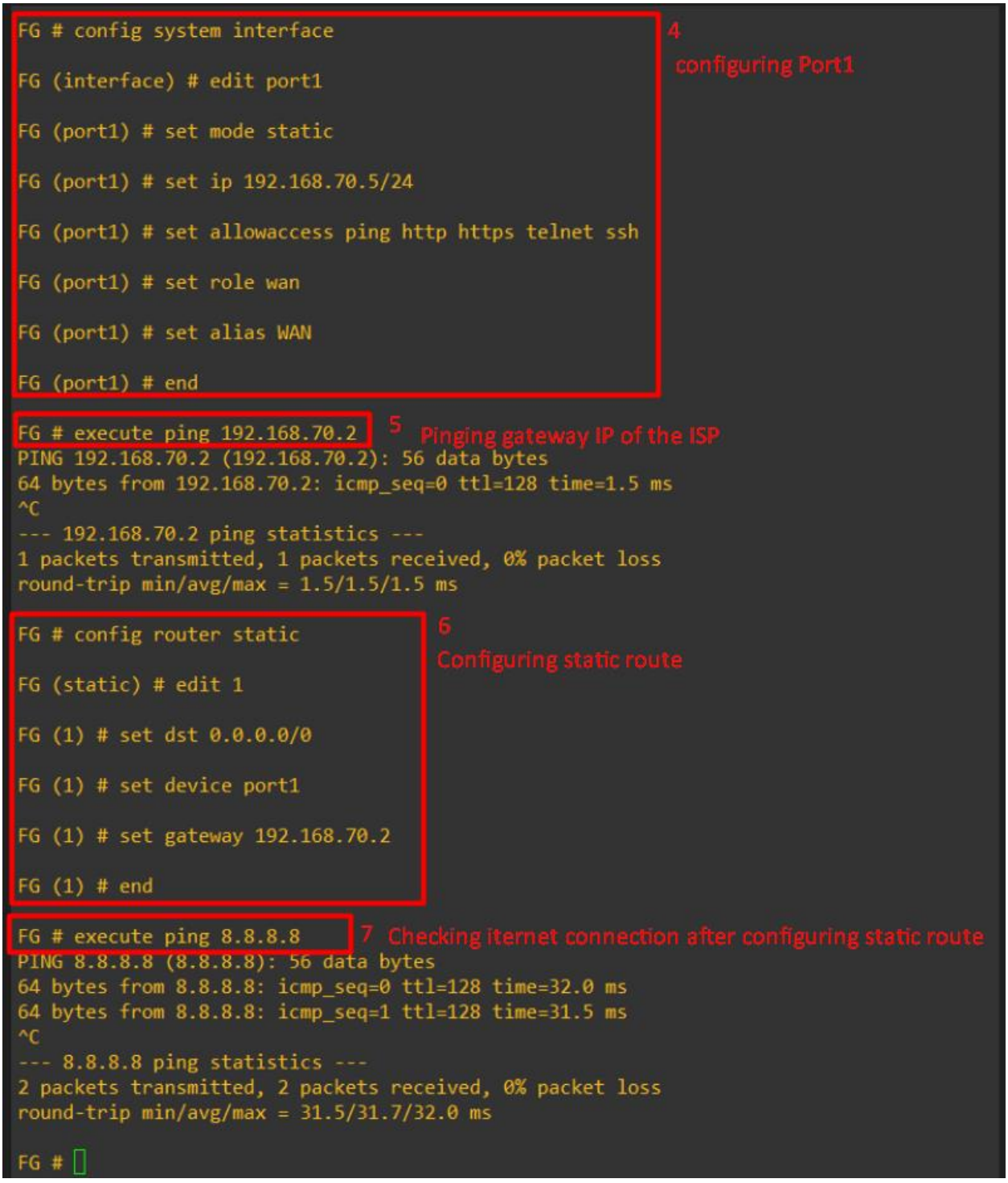


Figure 126 Assigning routes for WAN connection

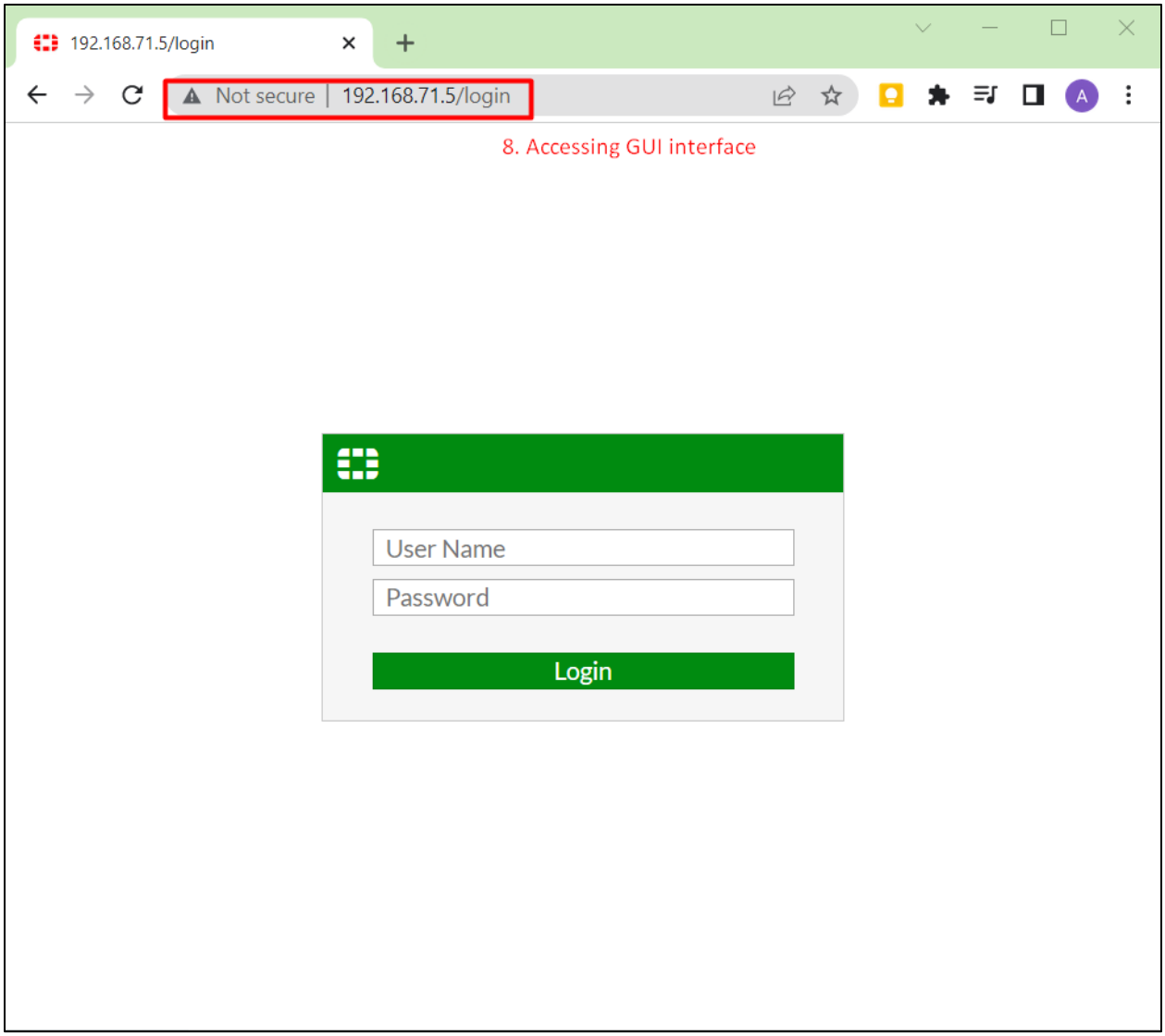


Figure 127 Accessing GUI

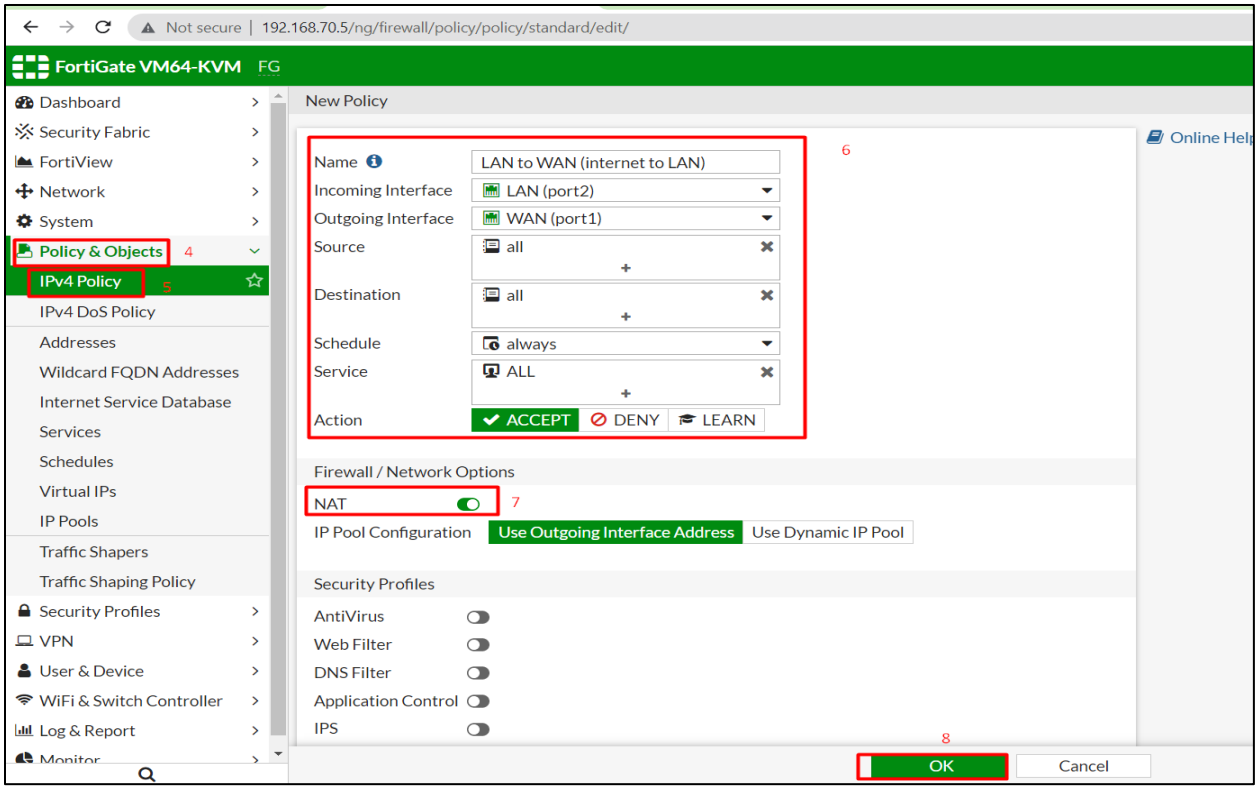


Figure 128 Creating policies to allow internet connection in internal LAN.

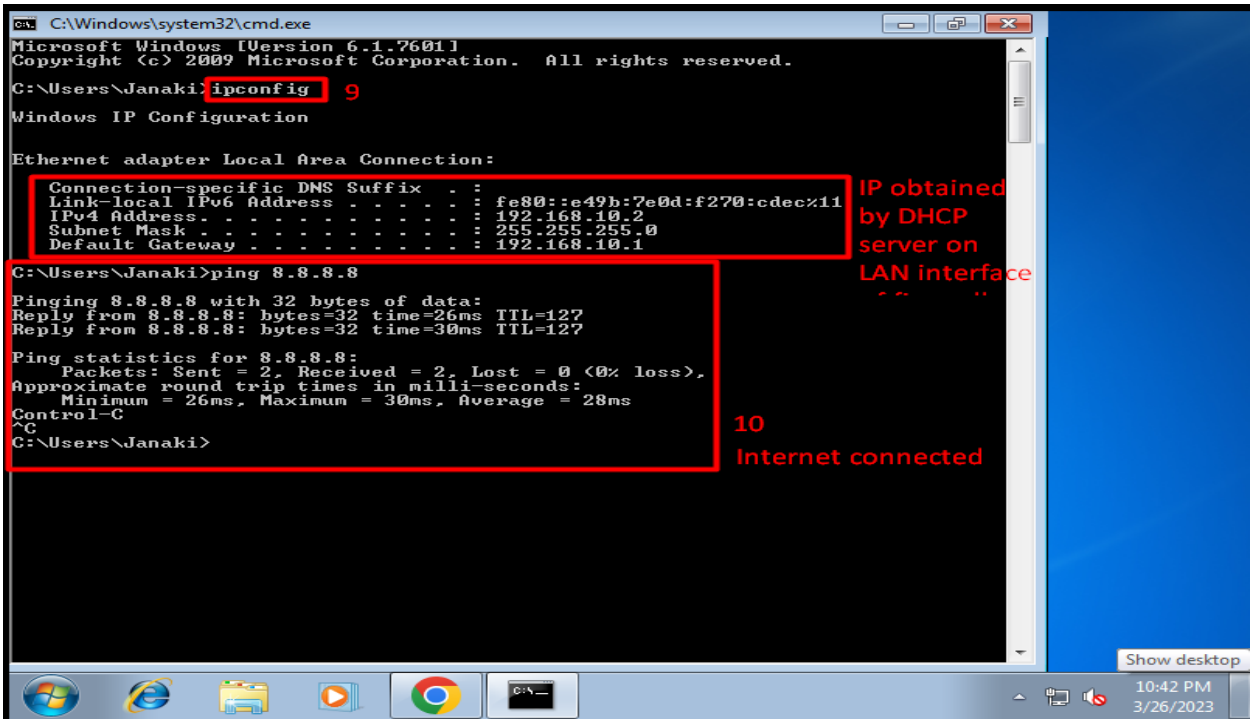


Figure 129 Dynamic IP address and internet connection in LAN PC.

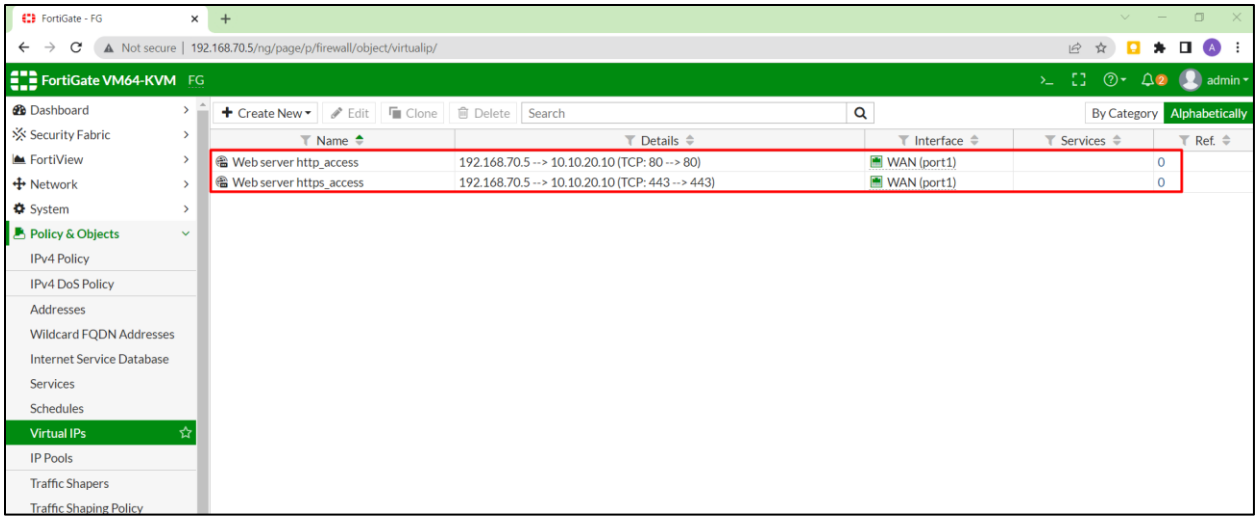


Figure 130 Creating virtual IPs for DMZ implementation.

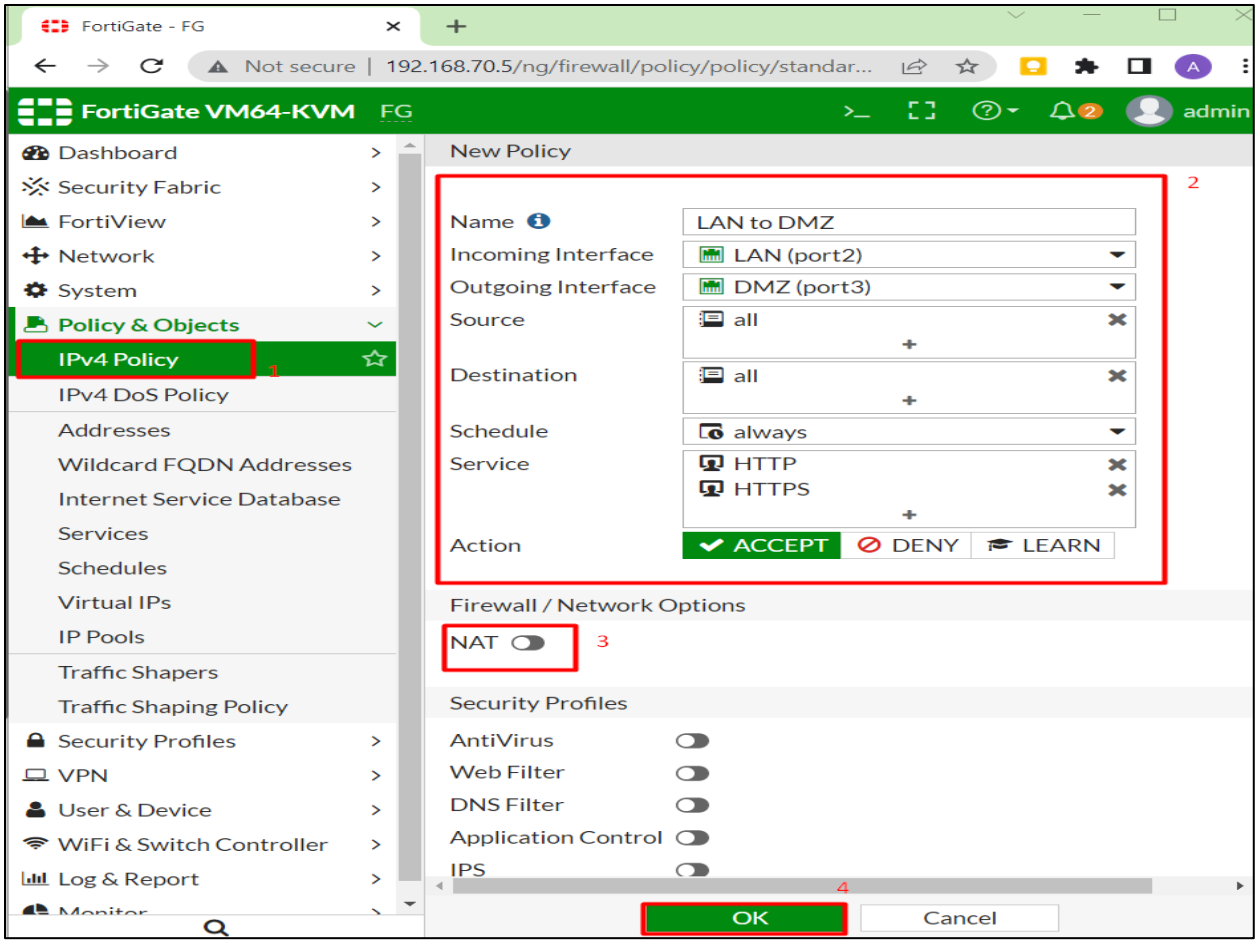


Figure 131 Firewall policy for DMZ implementation through LAN

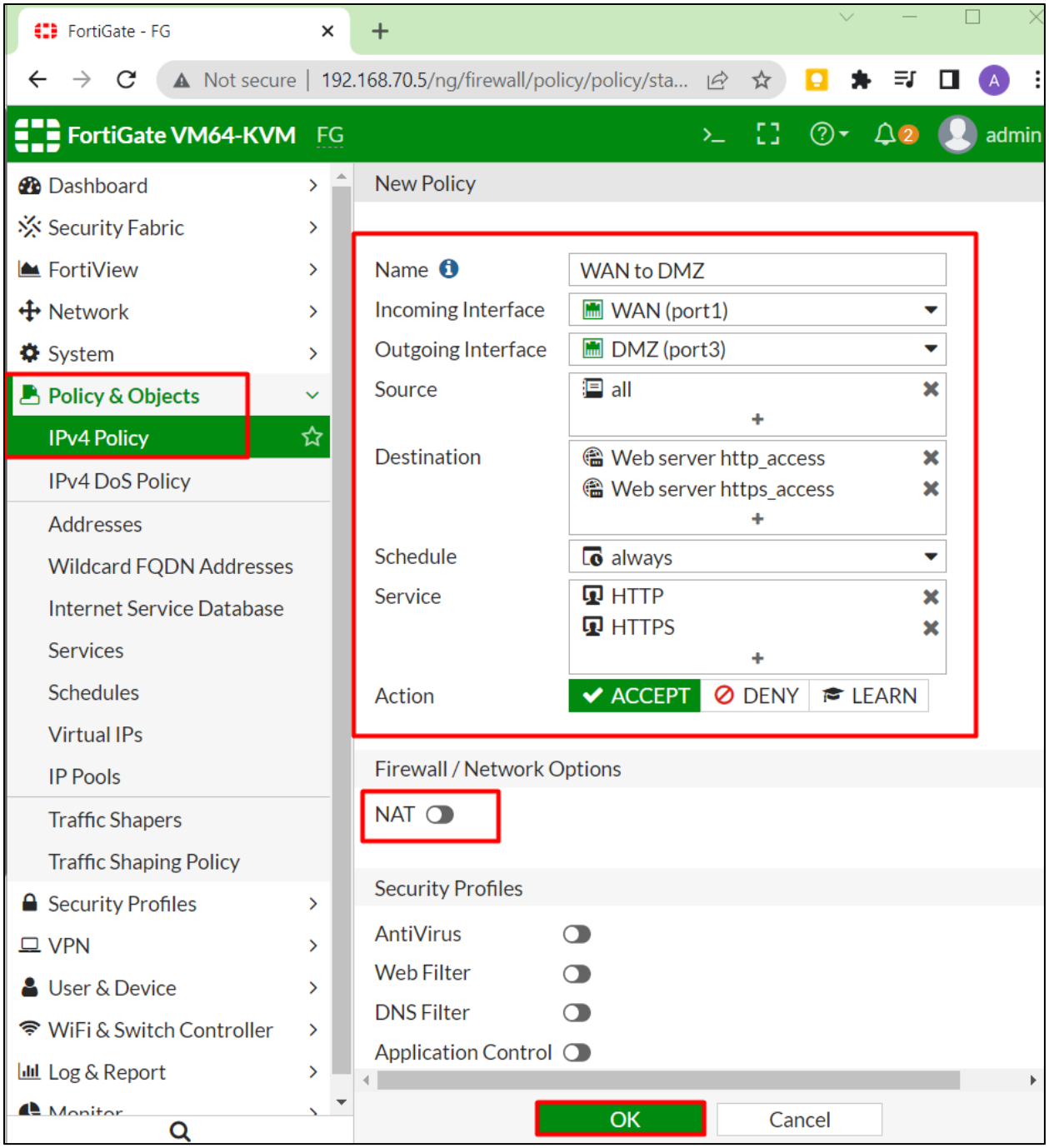


Figure 132 Firewall policy to implement DMZ through WAN

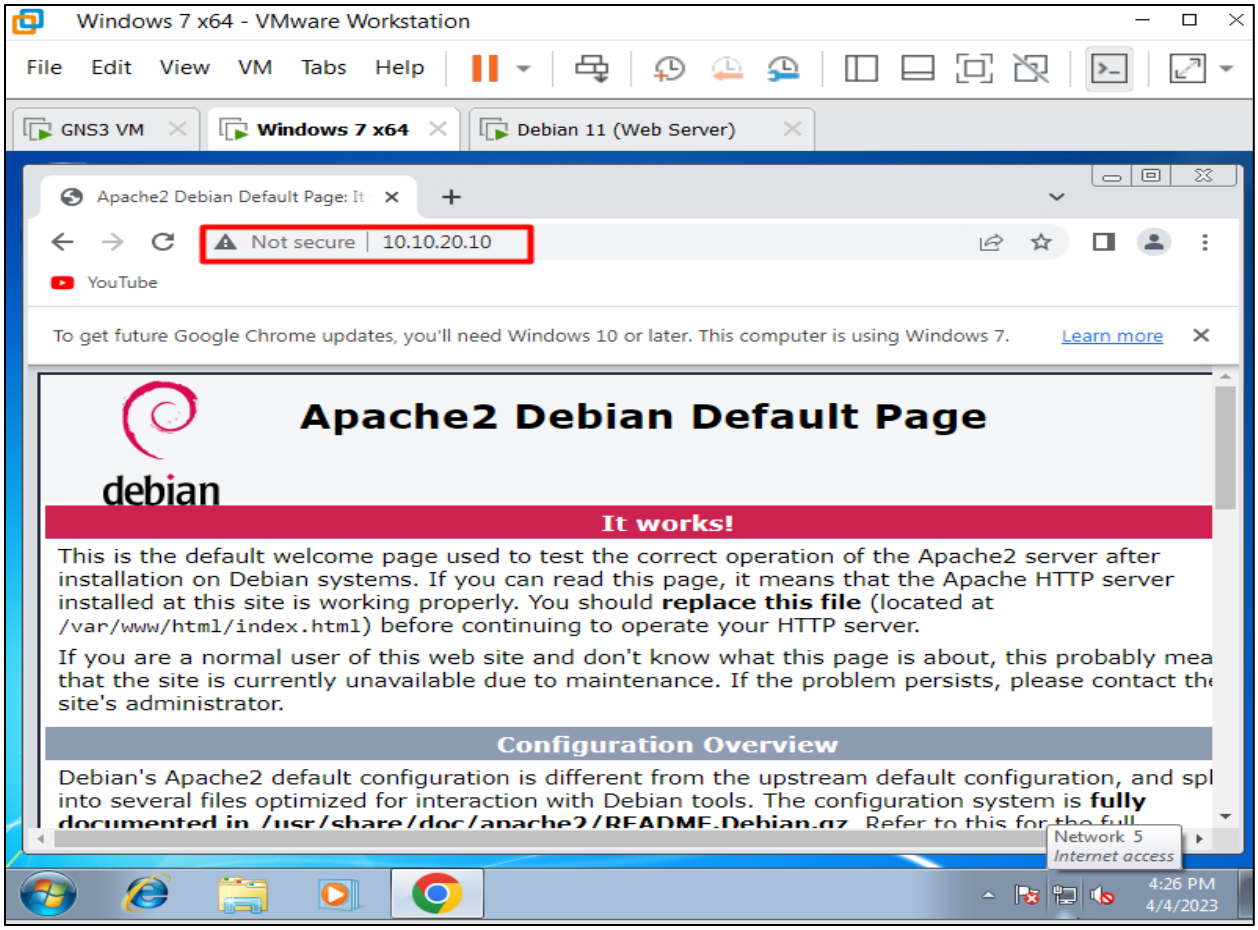


Figure 133 Internal user accessing web server in DMZ.

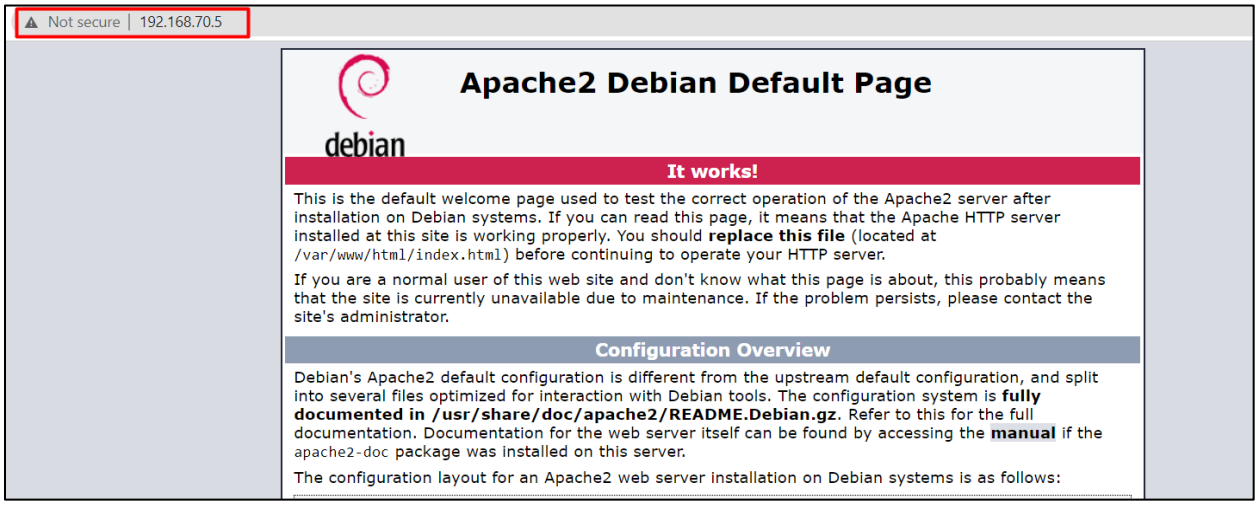


Figure 134 Internet/external users accesing web server in DMZ

8.4.2. External web server configuration (Debian 11)

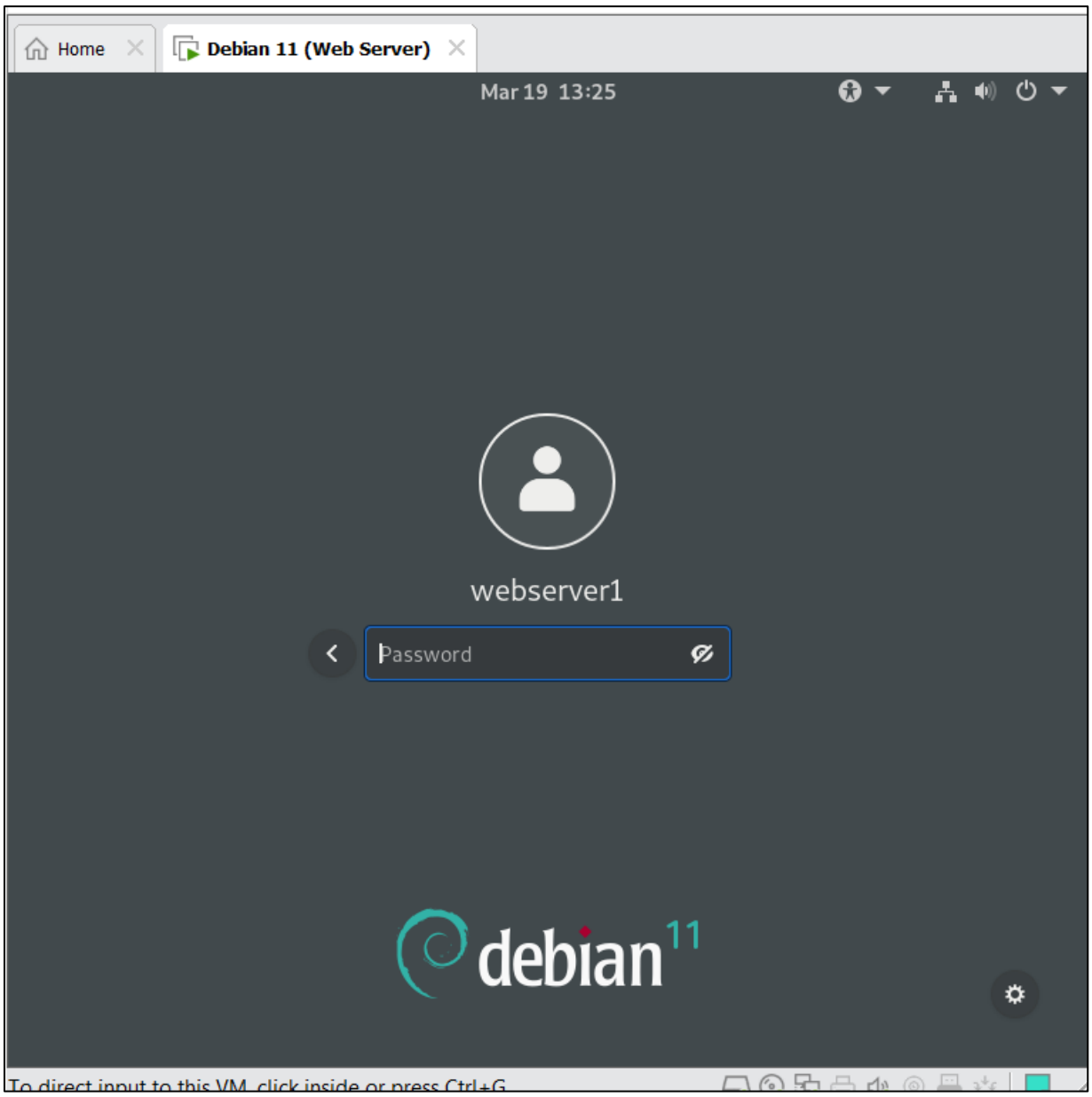


Figure 135 Debian 11

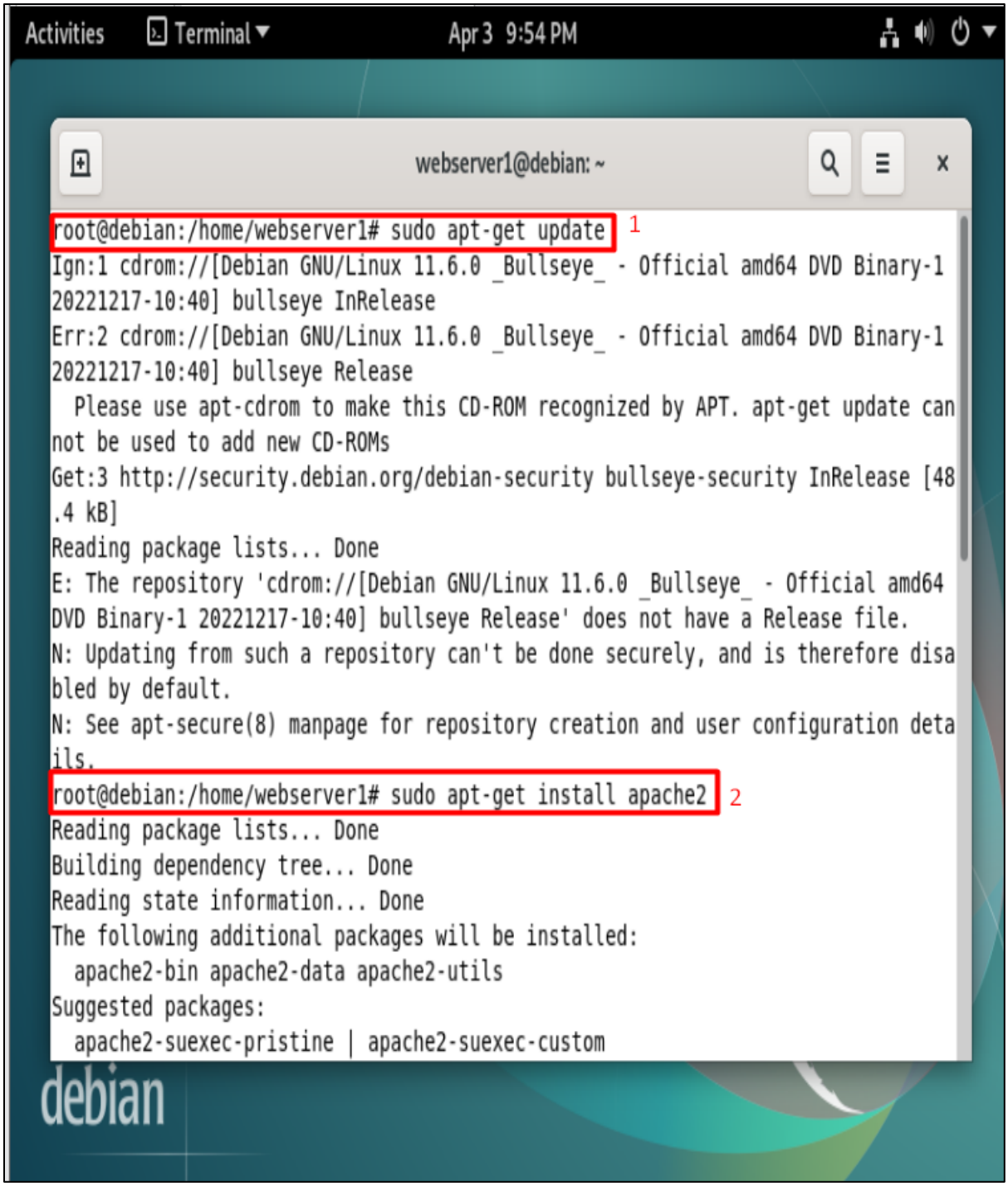


Figure 136 Apche2 installation

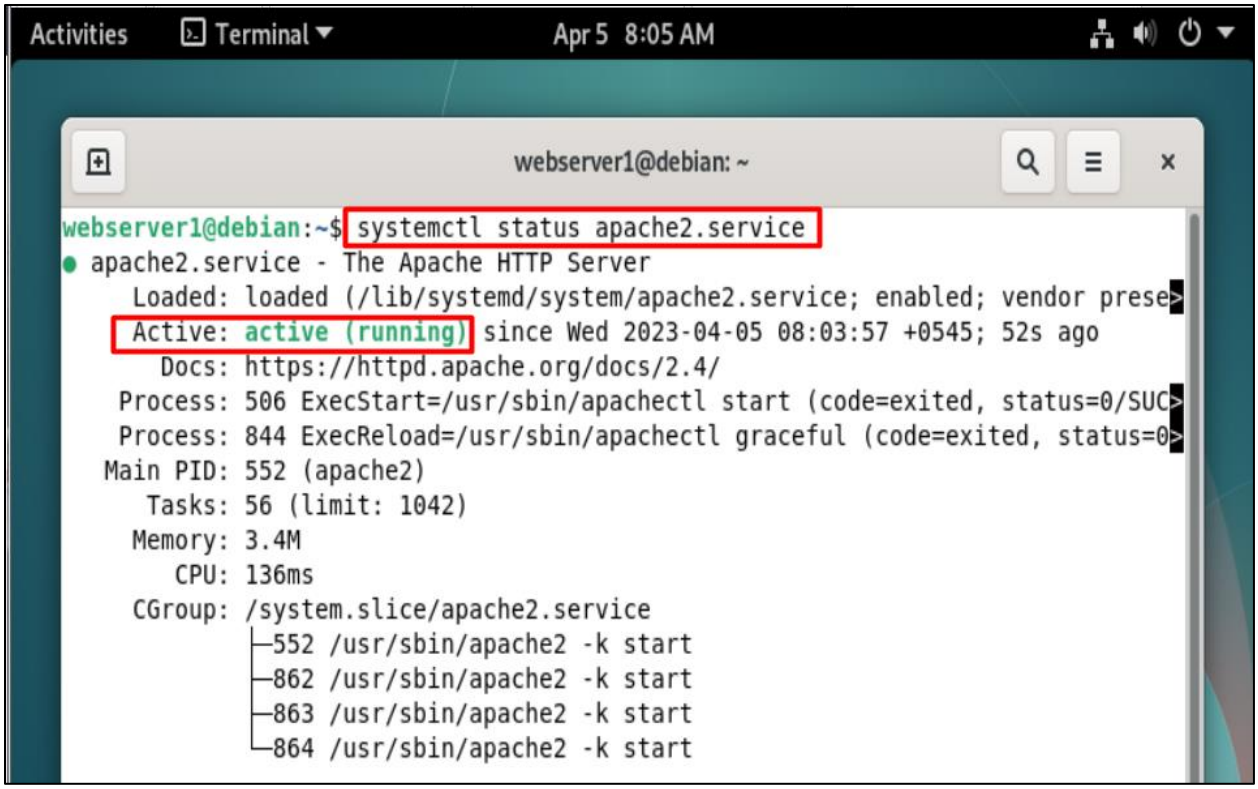


Figure 137 Checking web service status in Debian 11

8.4.3. Miktrotik router configuration

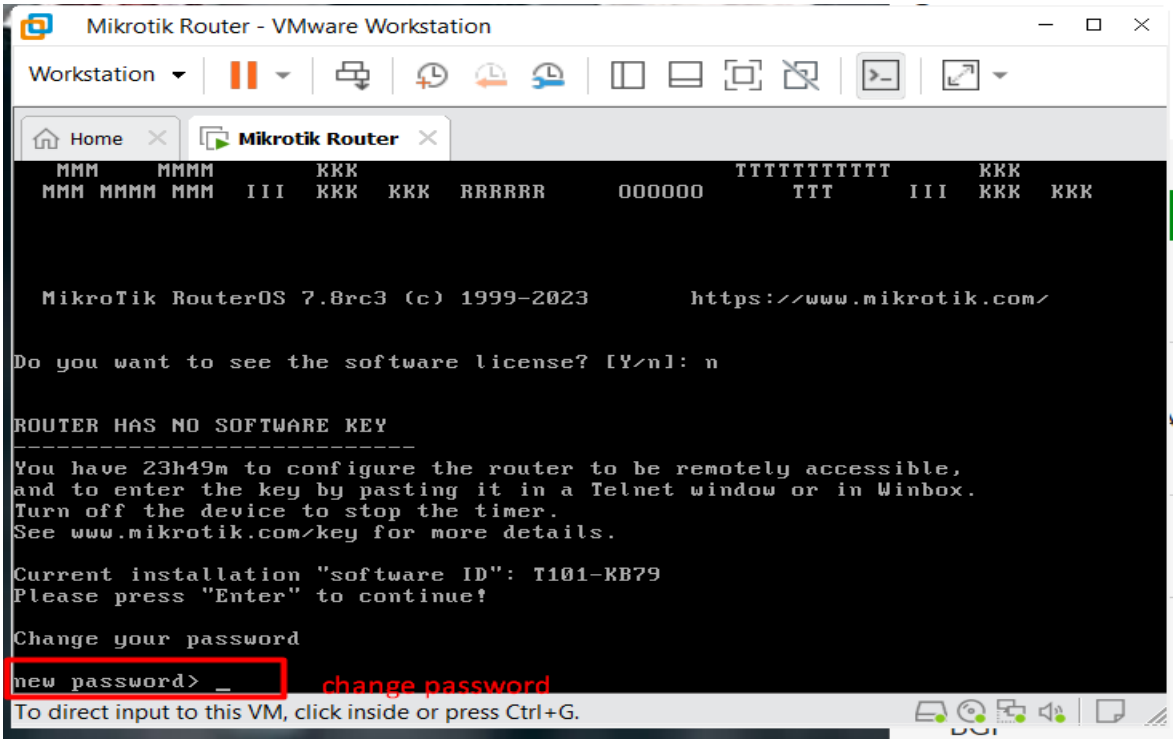


Figure 138 Miktrotik router installed.

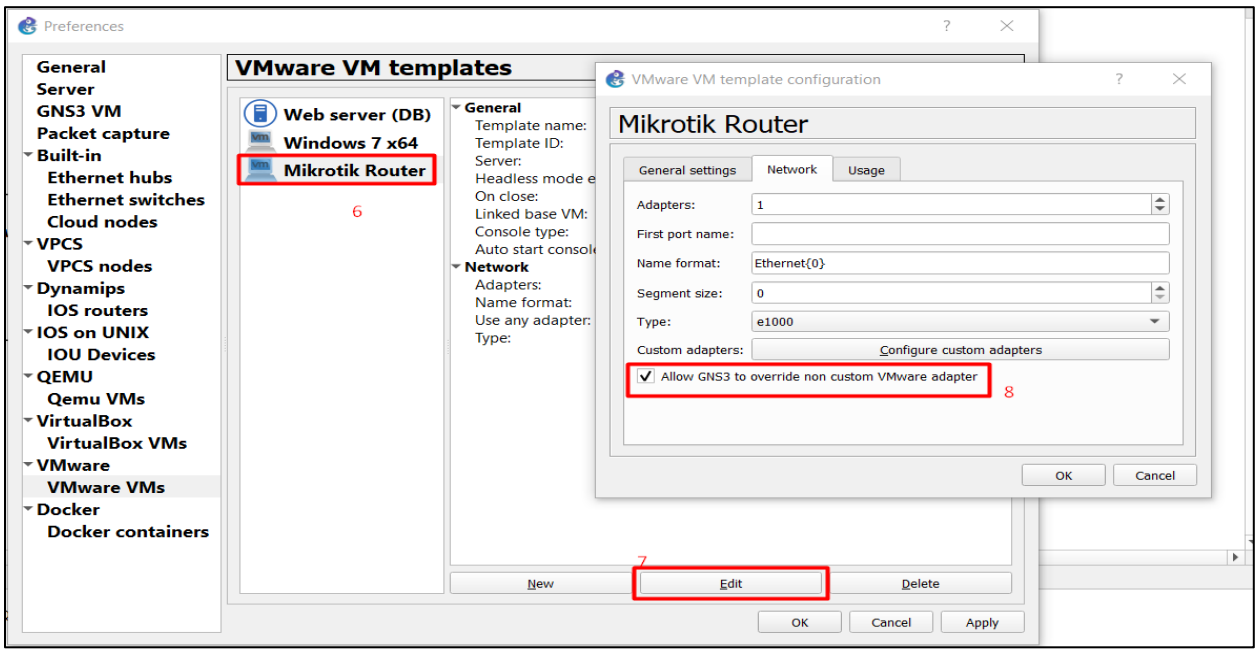


Figure 139 Adding Miktrotik as a VM node in GNS3.

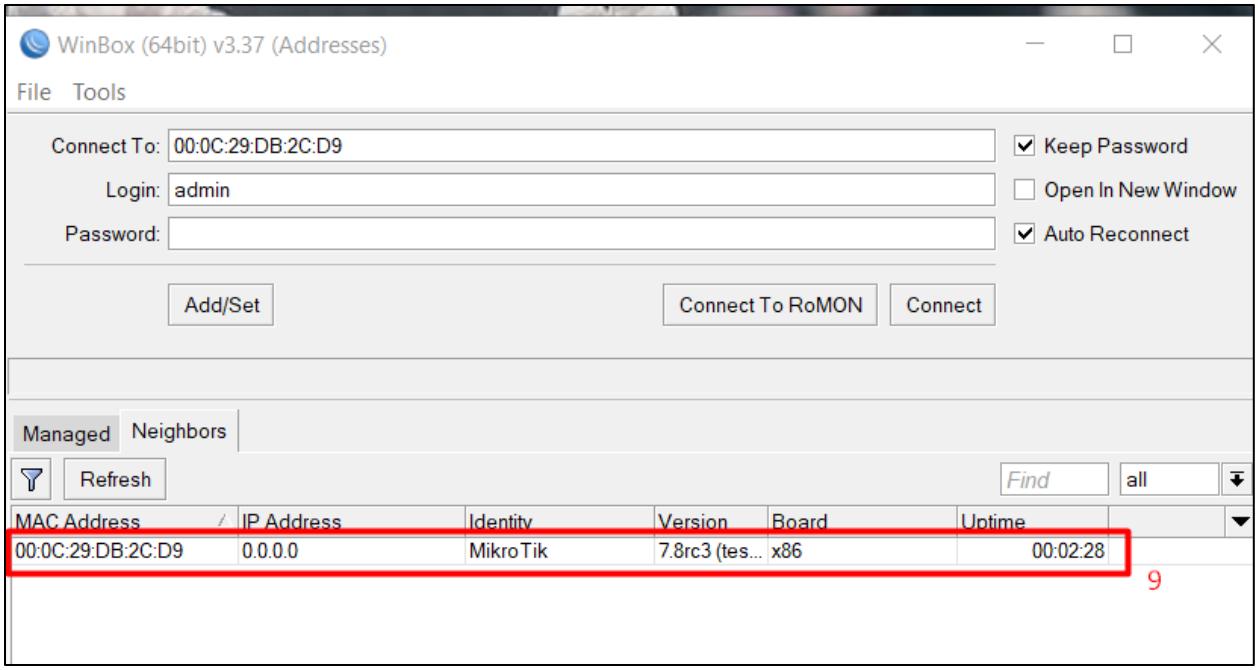


Figure 140 Accessing through Winbox

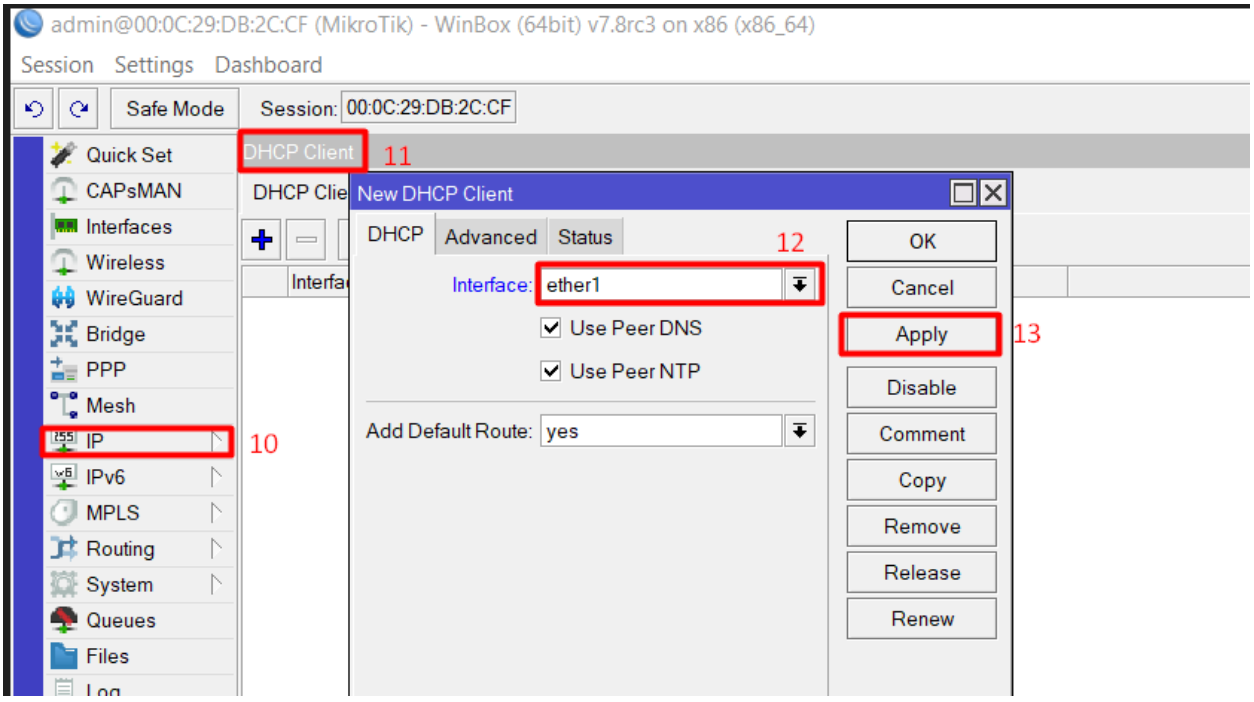


Figure 141 Enabling DHCP client.

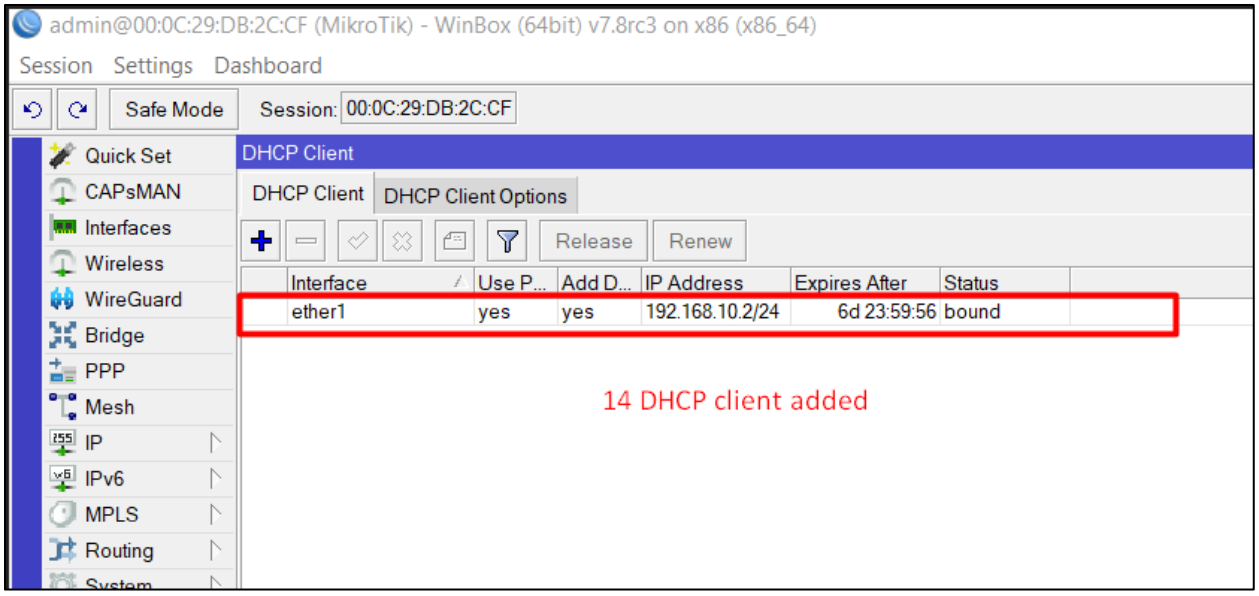


Figure 142 DHCP client added.

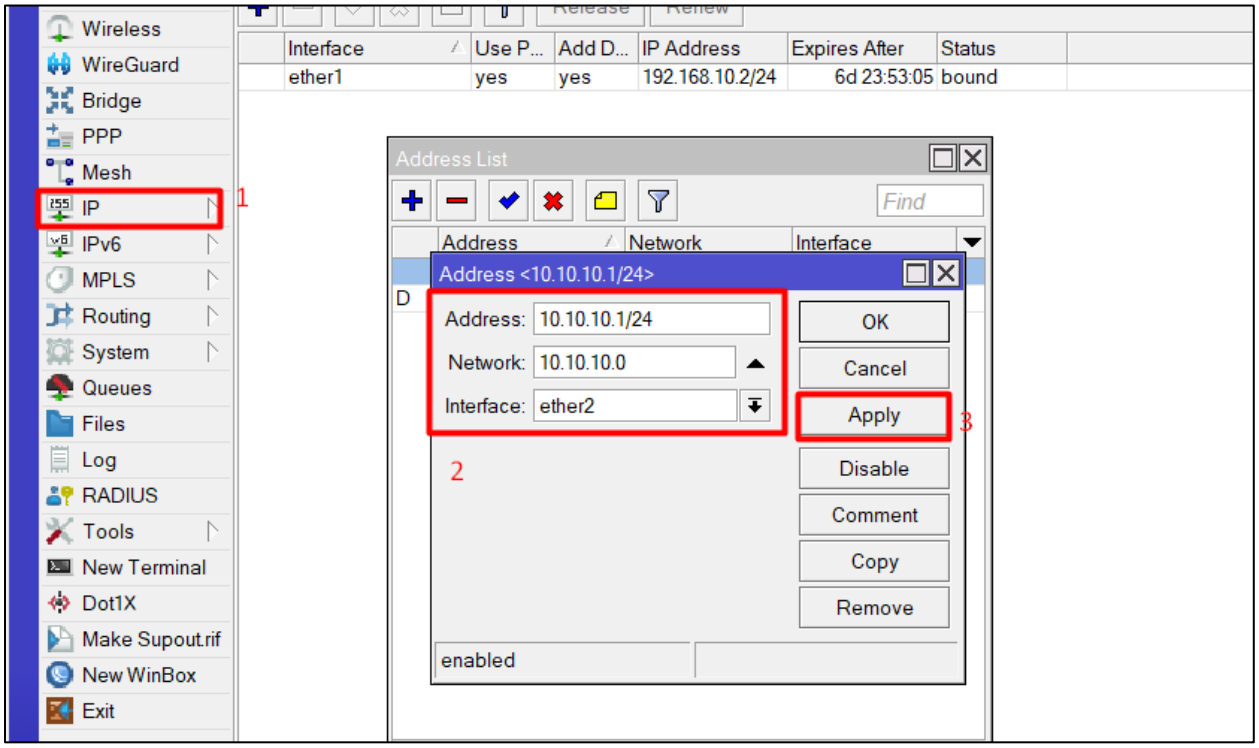


Figure 143 Adding IP address on Ether 2

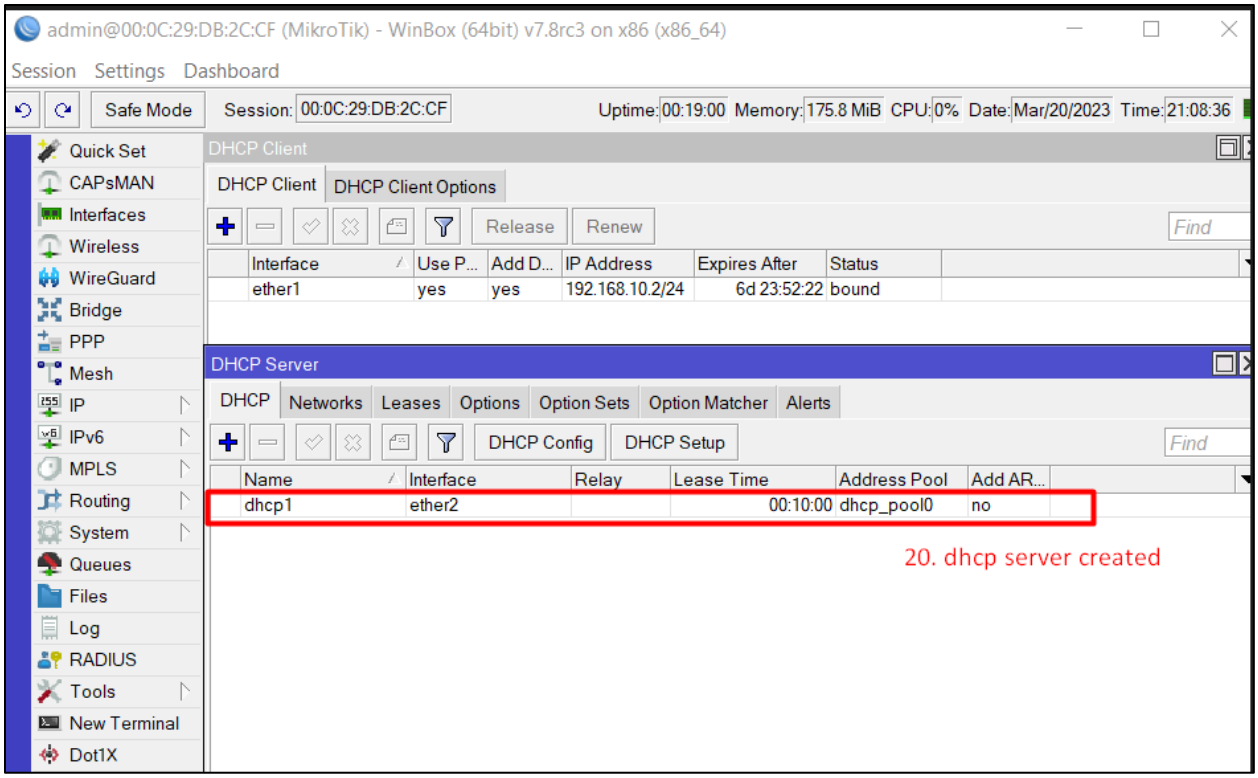


Figure 144 DHCP server created on Ether2.

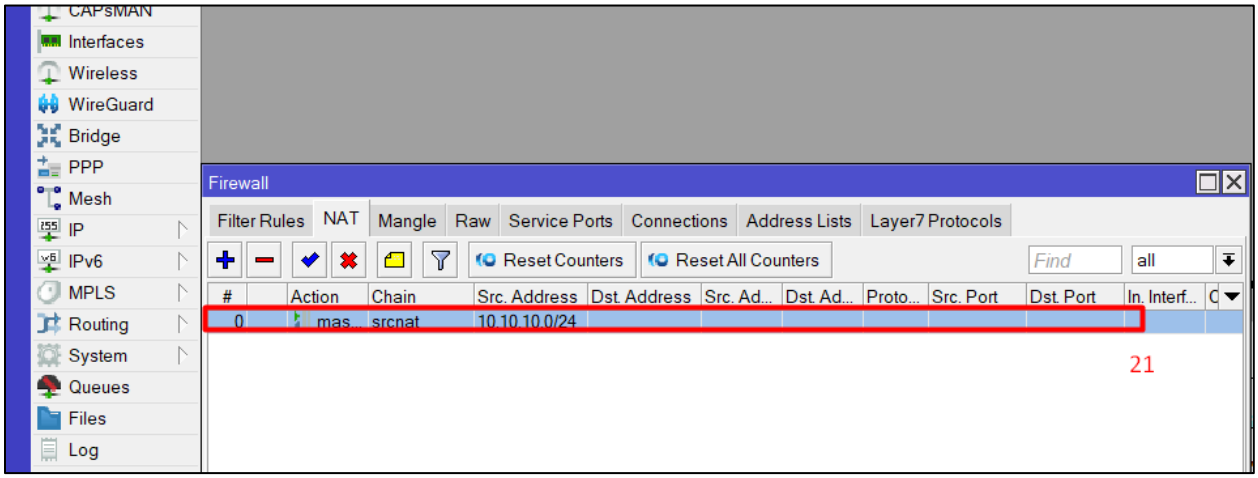


Figure 145 Configure source Nat on Ether2.

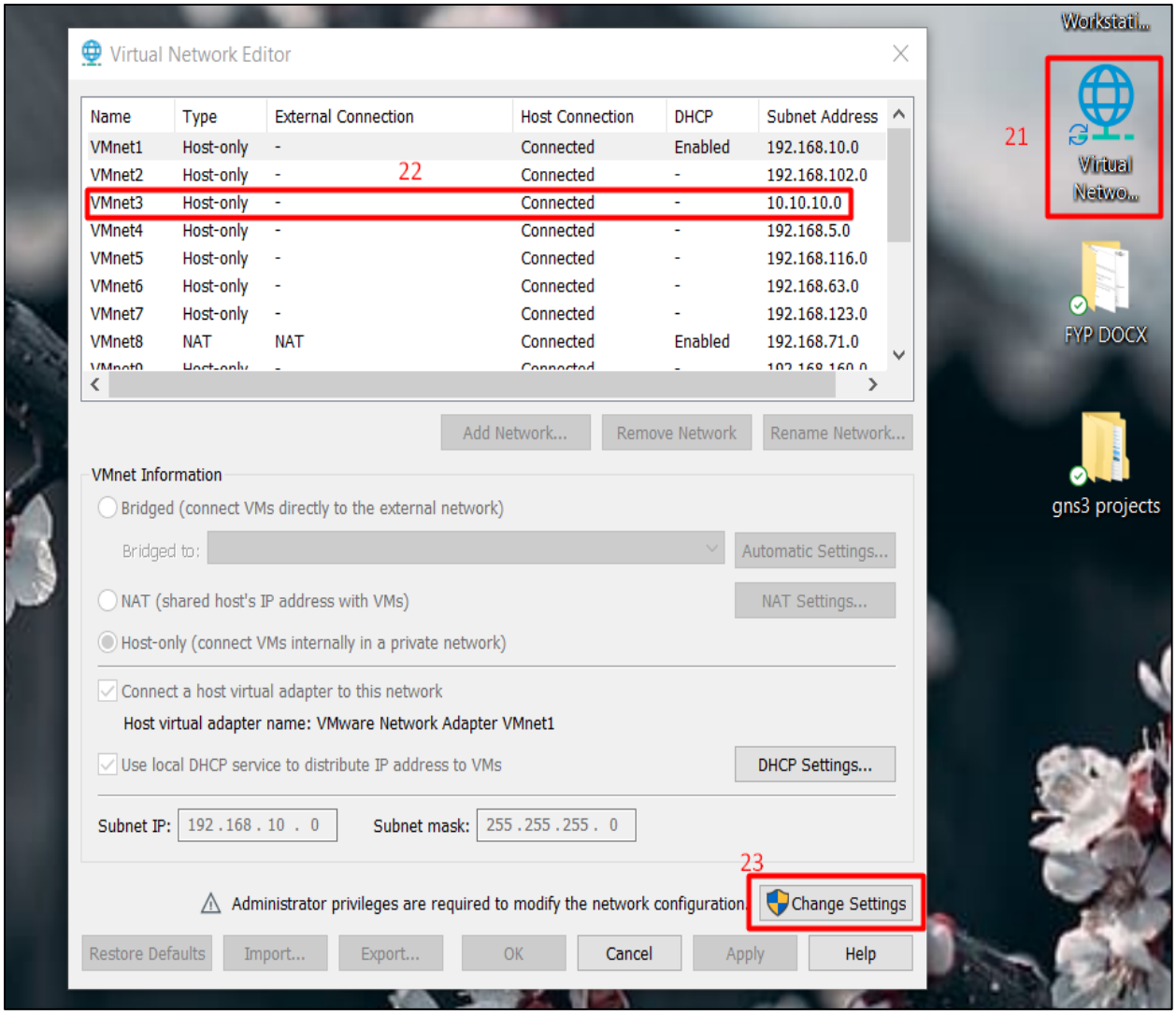


Figure 146 Edit virtual Adapter to connect ESXi.

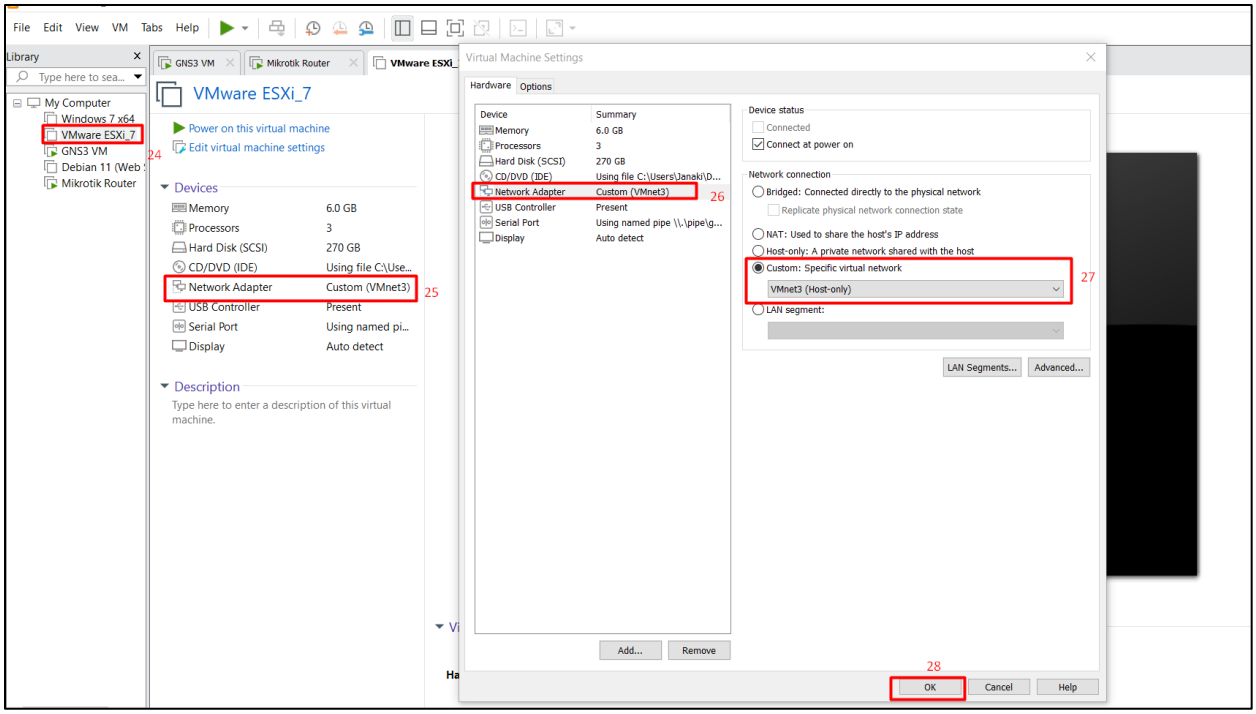


Figure 147 Changing ESXi network adapter to custom

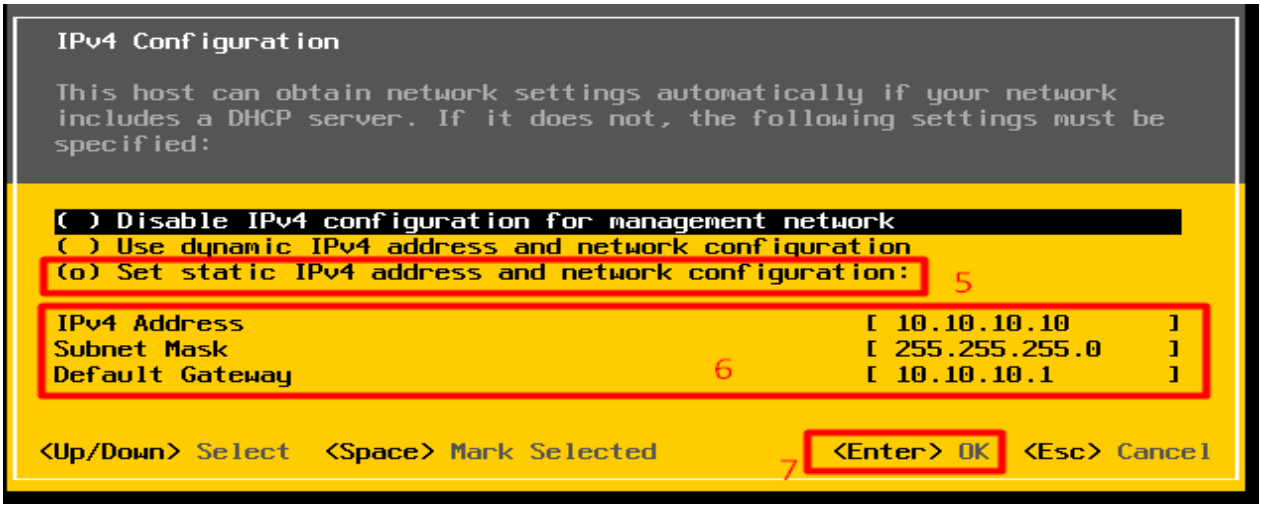


Figure 148 Assigning static IP address of ESXi.

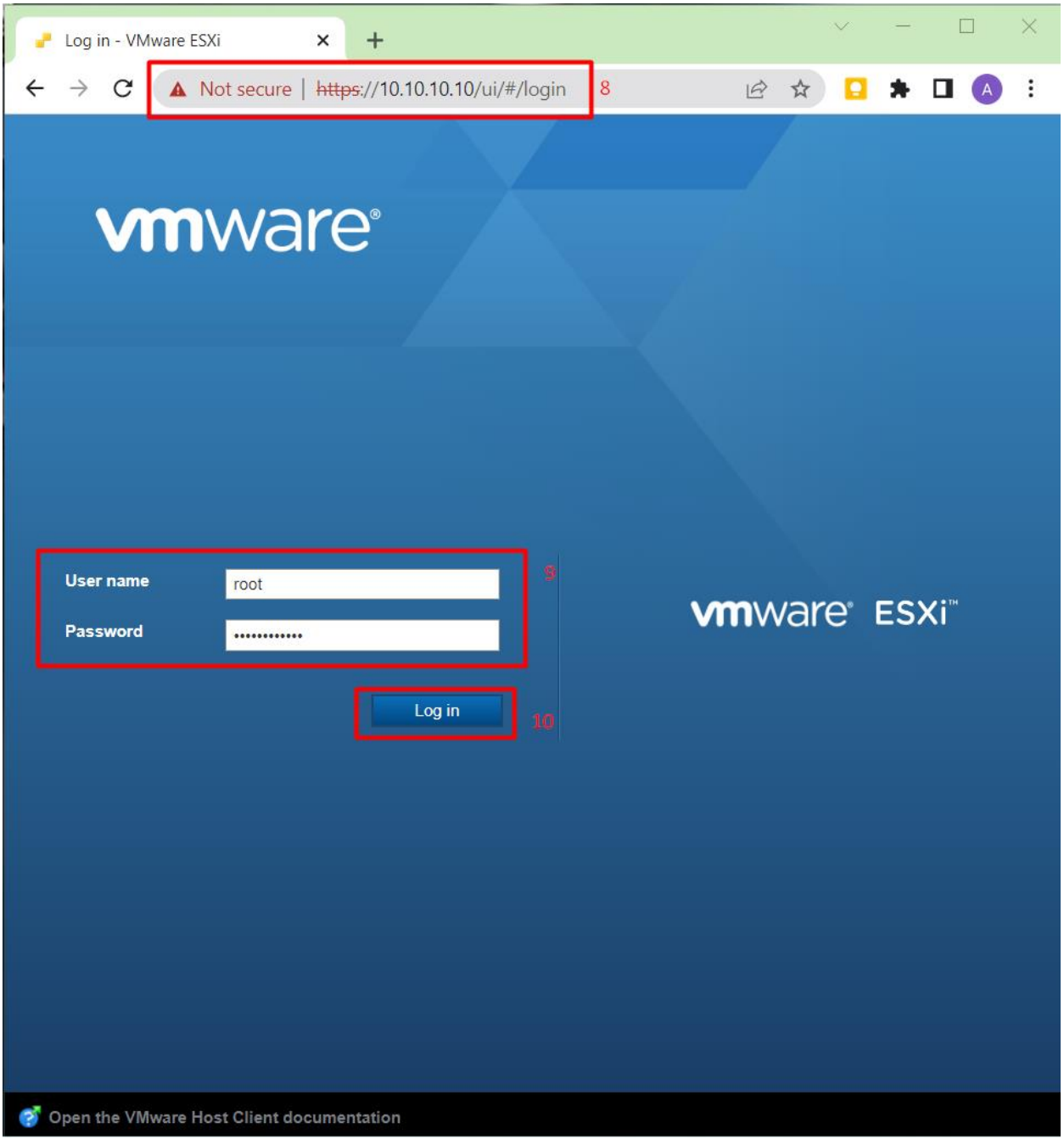


Figure 149 Accessing GUI of ESXi

8.4.4. VMware ESXi configuration

8.4.4.1. Increase data store of ESXi.

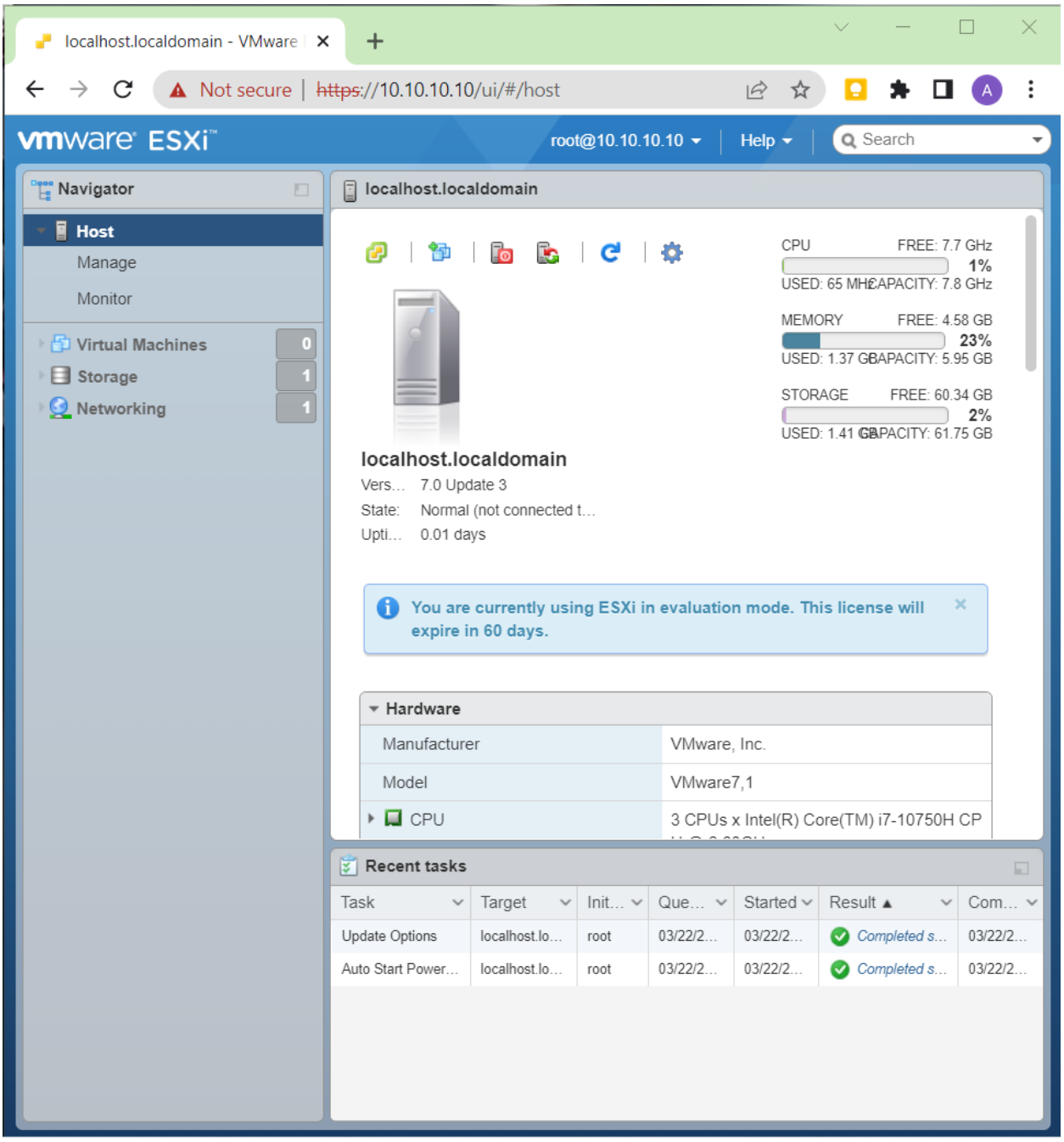


Figure 150 Accessing ESXi host interface for further tasks.

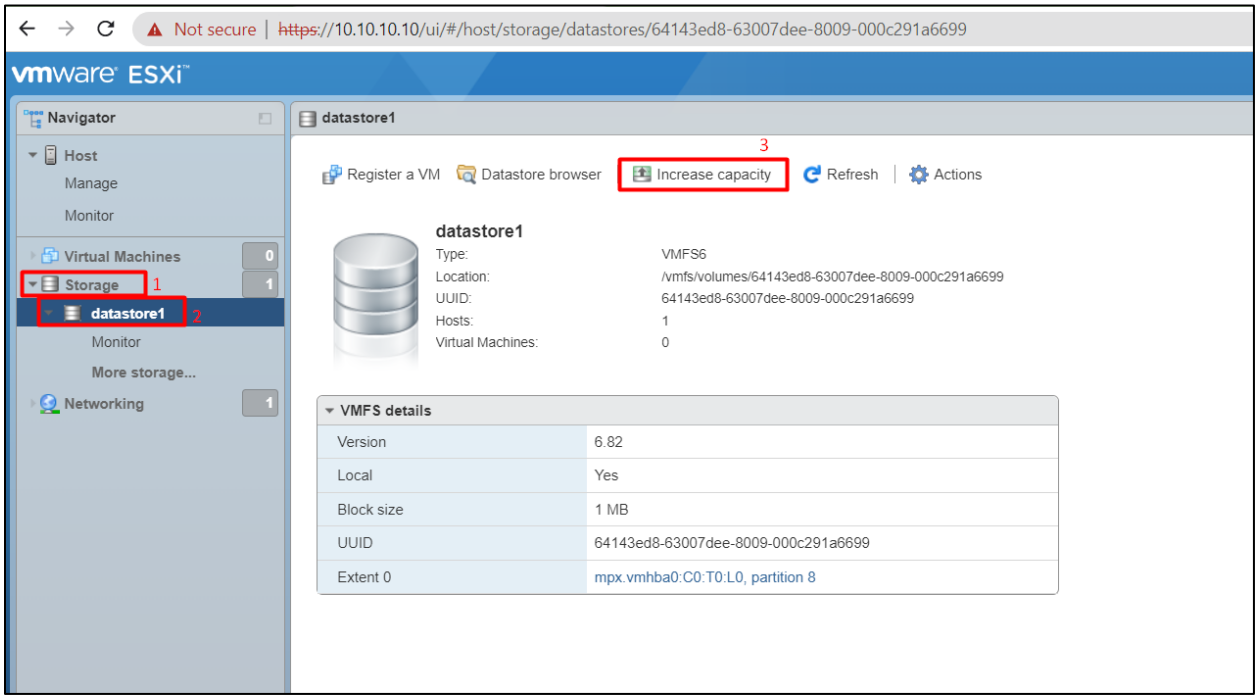


Figure 151 Increasing datastore capacity.

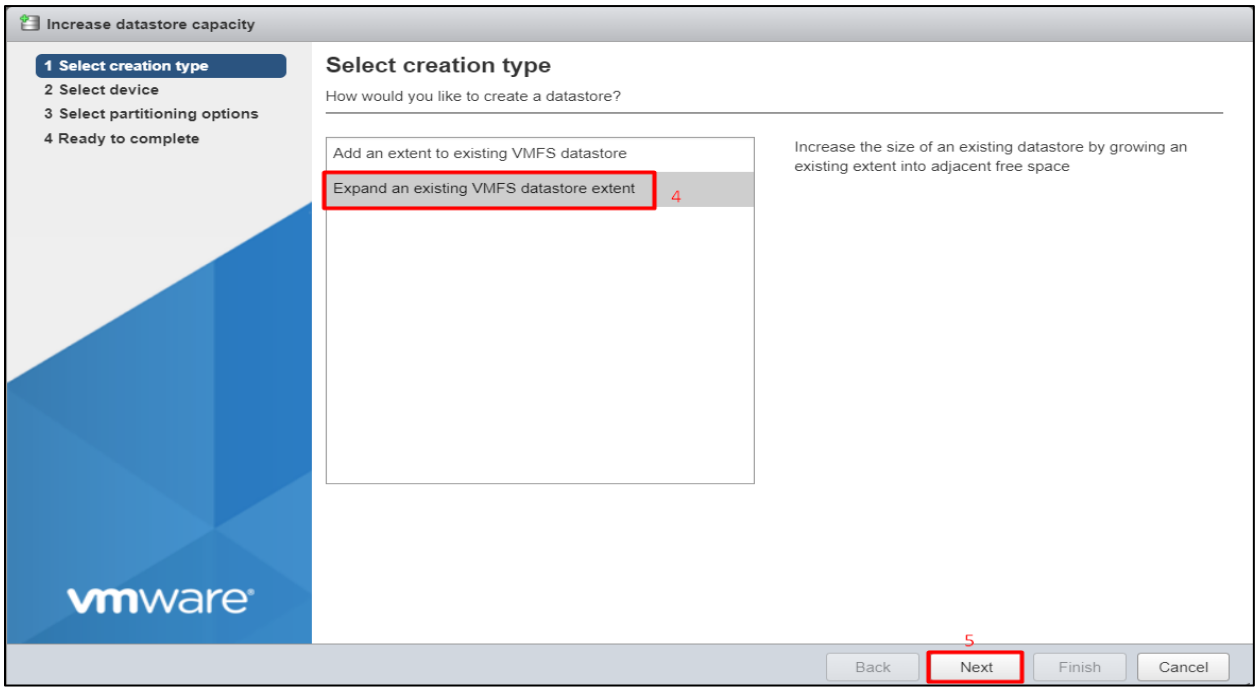


Figure 152 Increasing data store capacity (2)

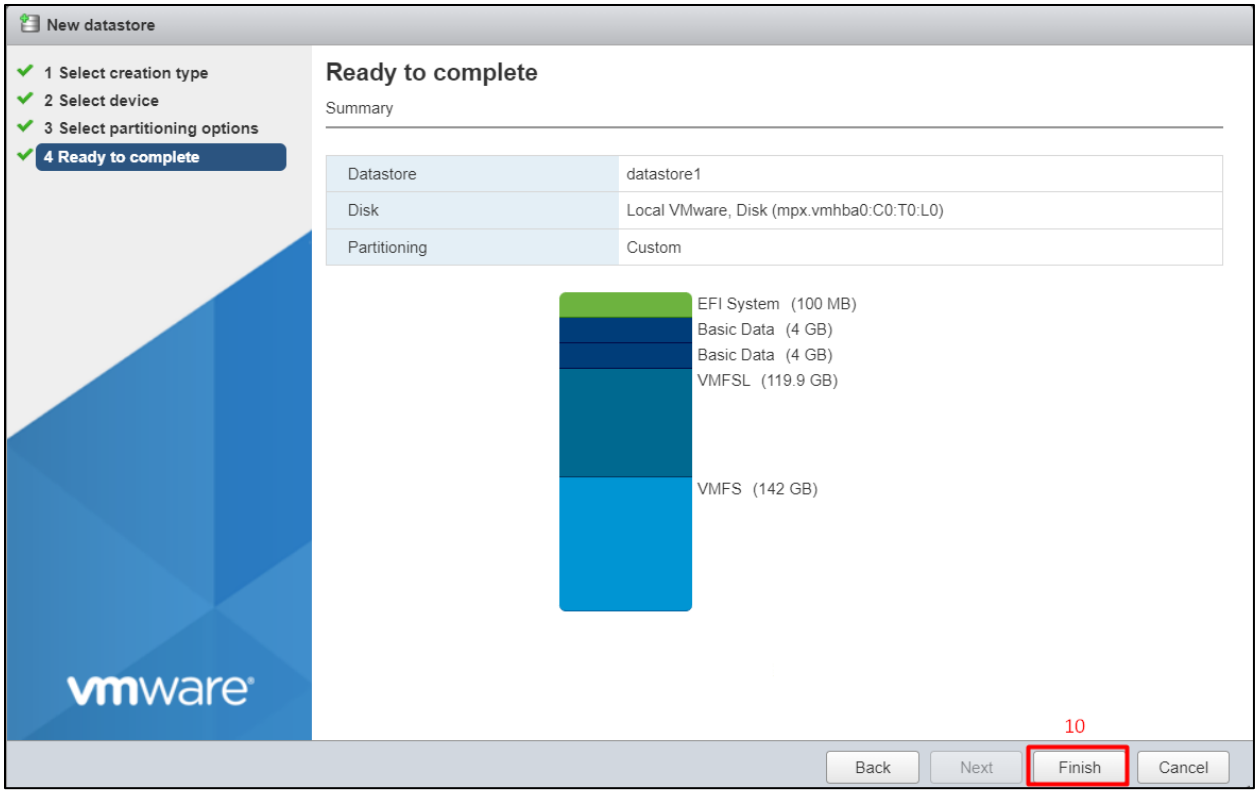


Figure 153 Increasing datastore capacity (3)

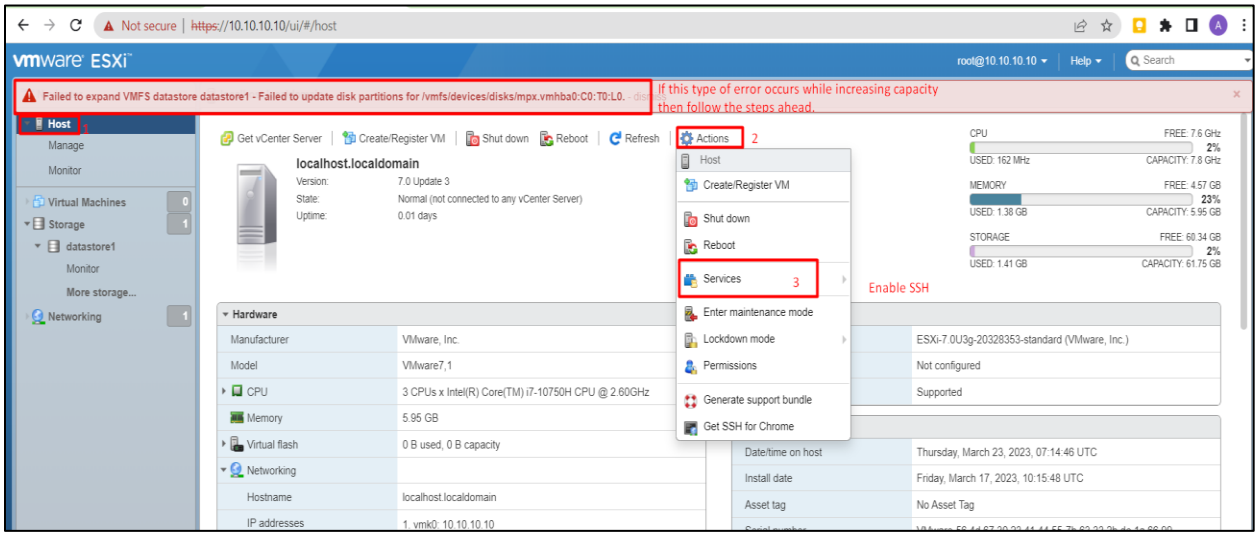


Figure 154 Increasing datastore capacity (4).

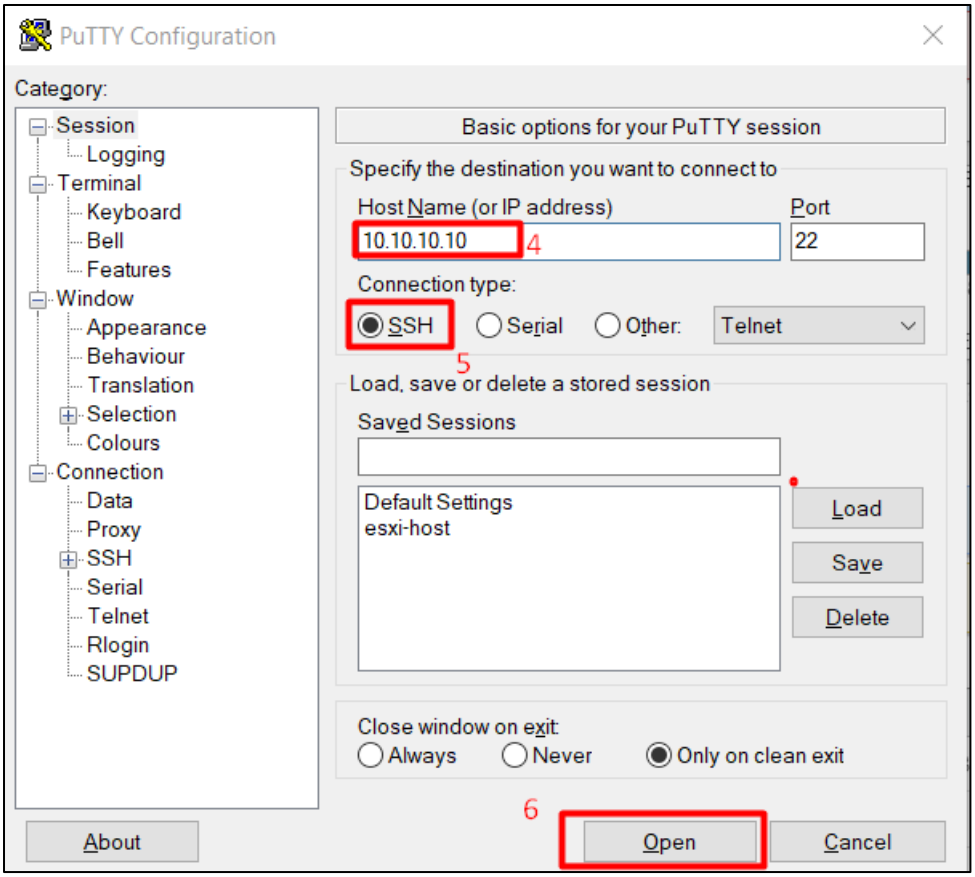


Figure 155 Enabling SSH to increase data store of ESXi.

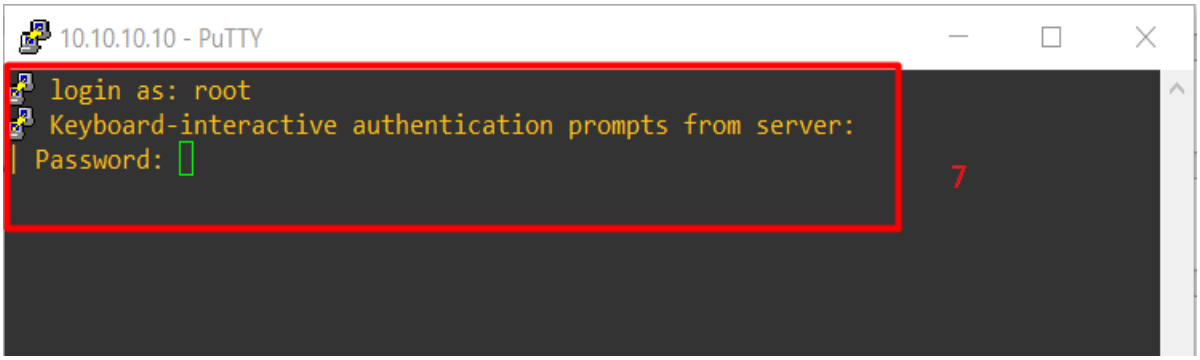


Figure 156 Logging in ESXi SSH.

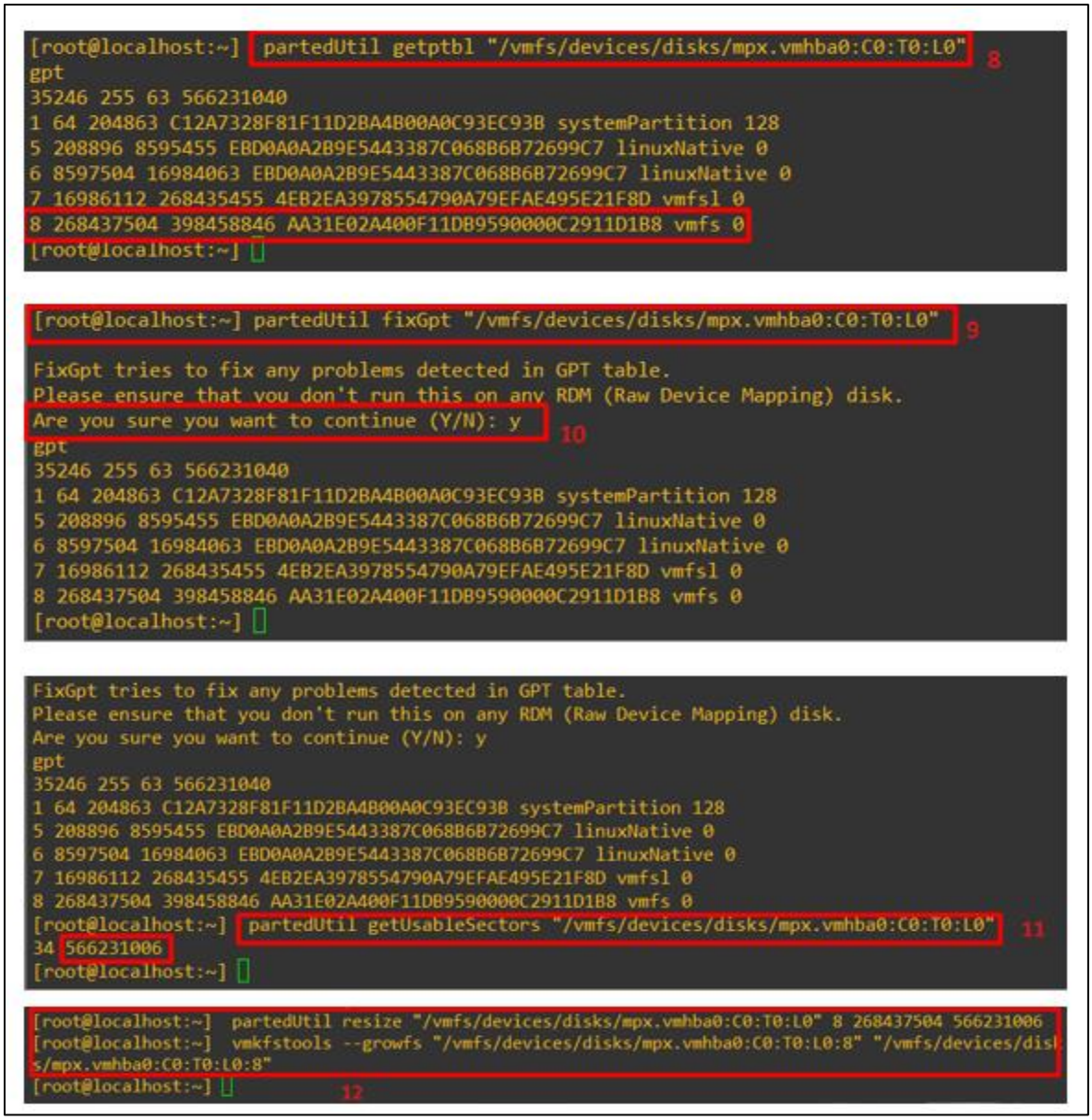


Figure 157 Commands to increase datastore of ESXi.

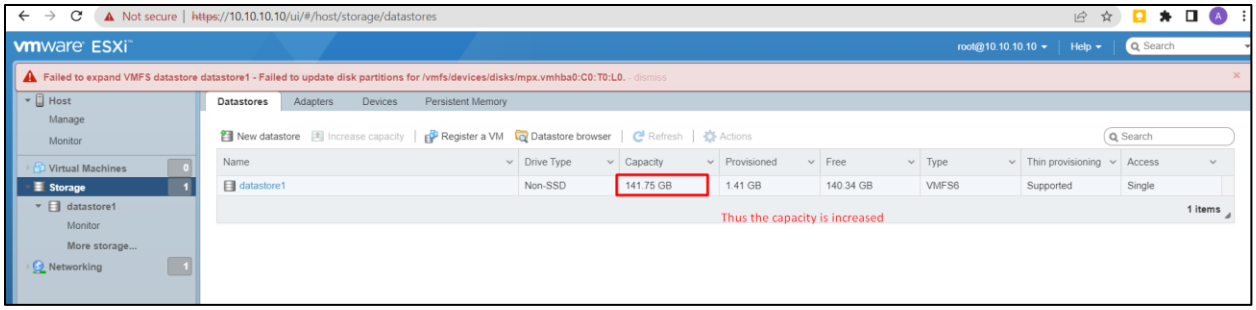


Figure 158 The datastore's capacity increased successfully.

8.4.4.2. Domain controller configuration

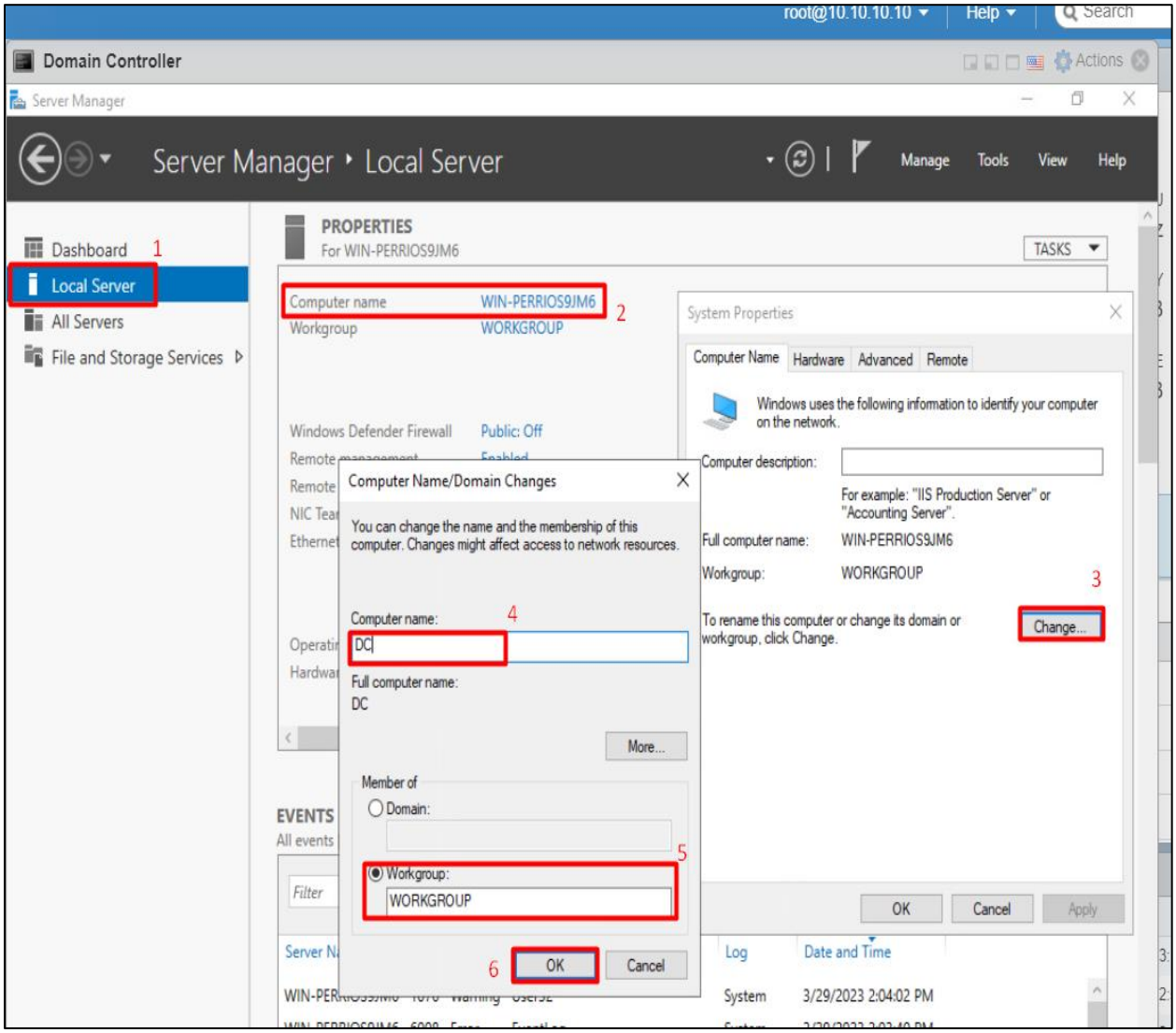


Figure 159 Providing server name.

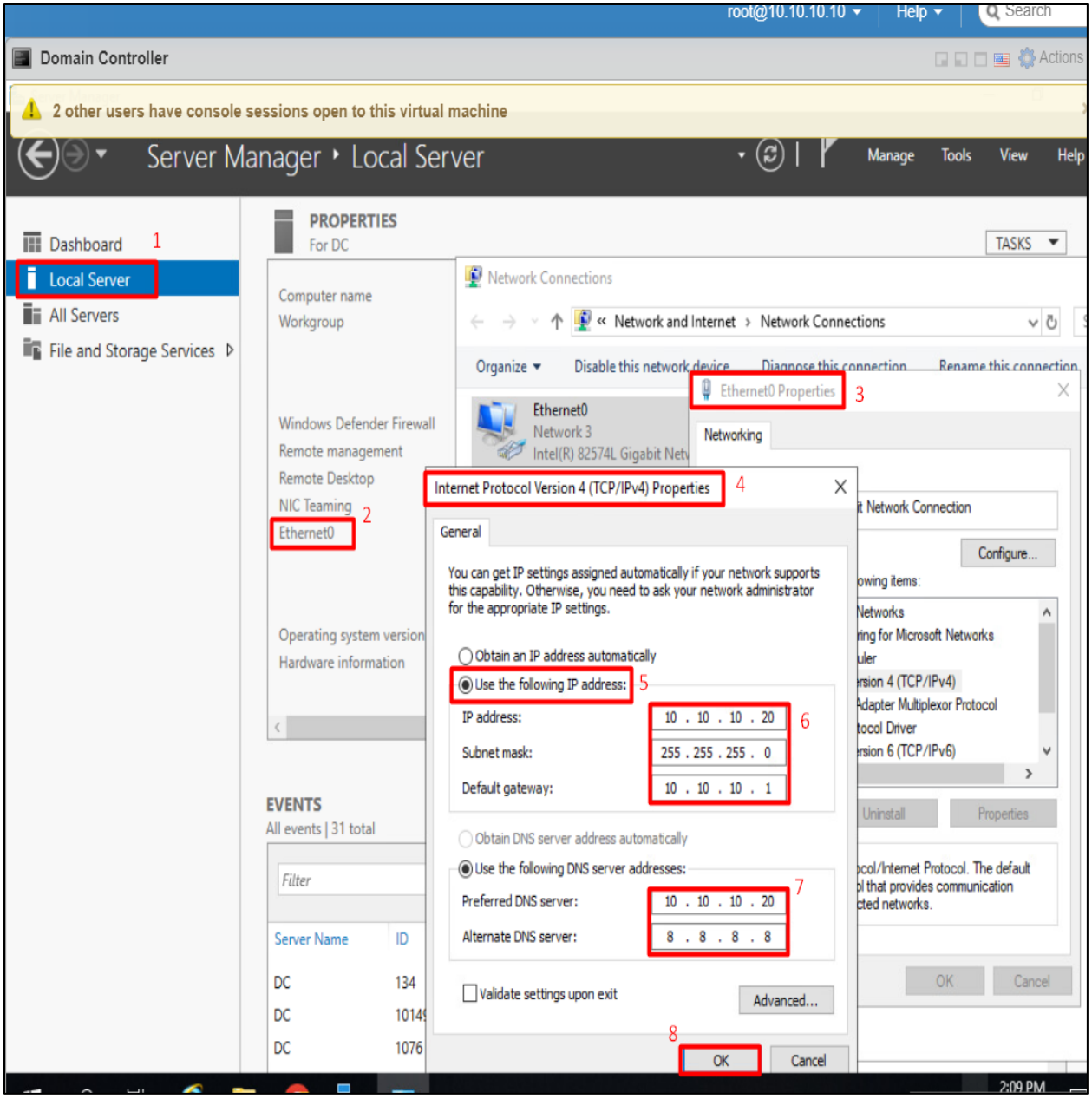


Figure 160 Assigning static IP address and DNS.

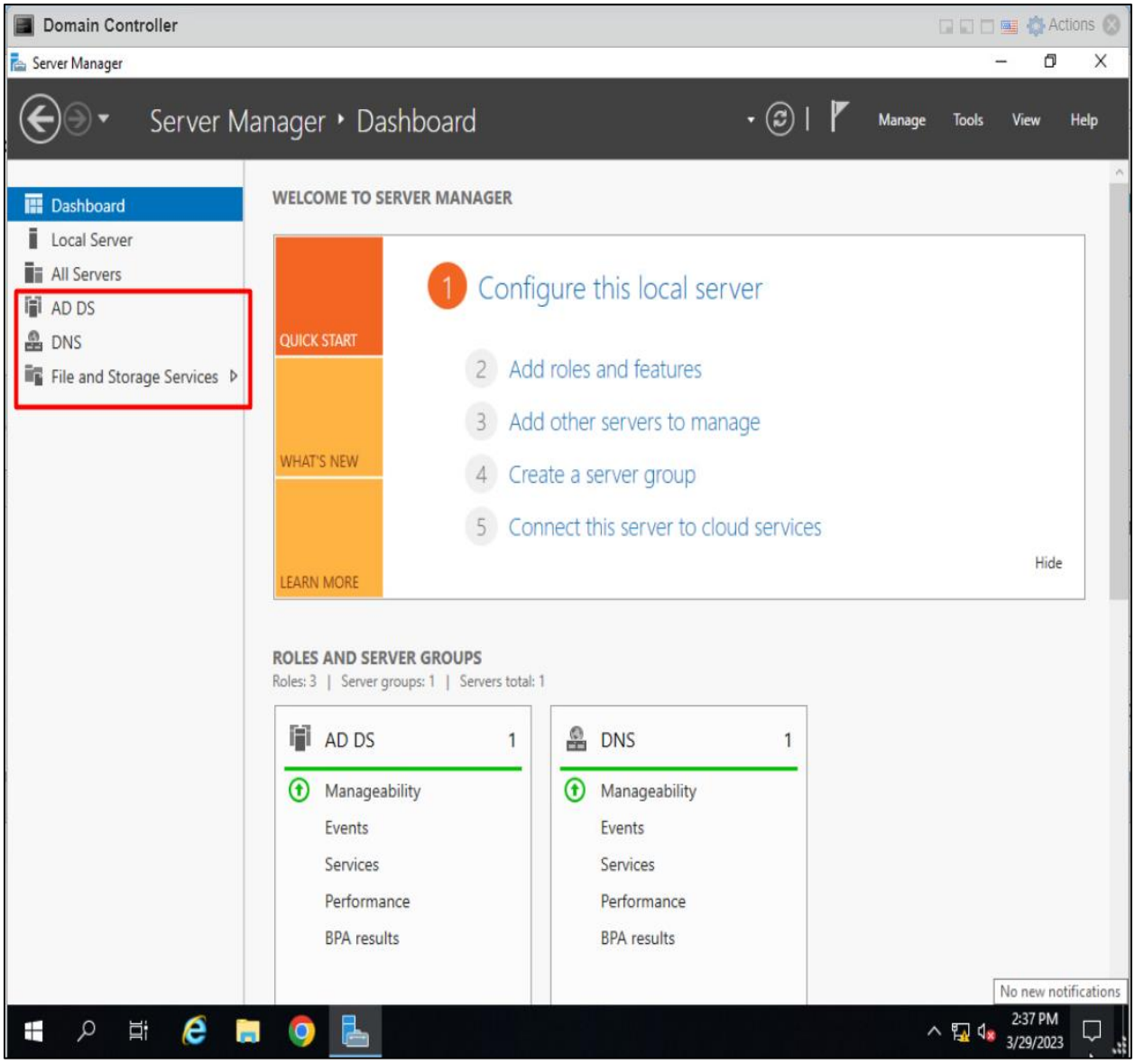


Figure 161 ADDS role installed.

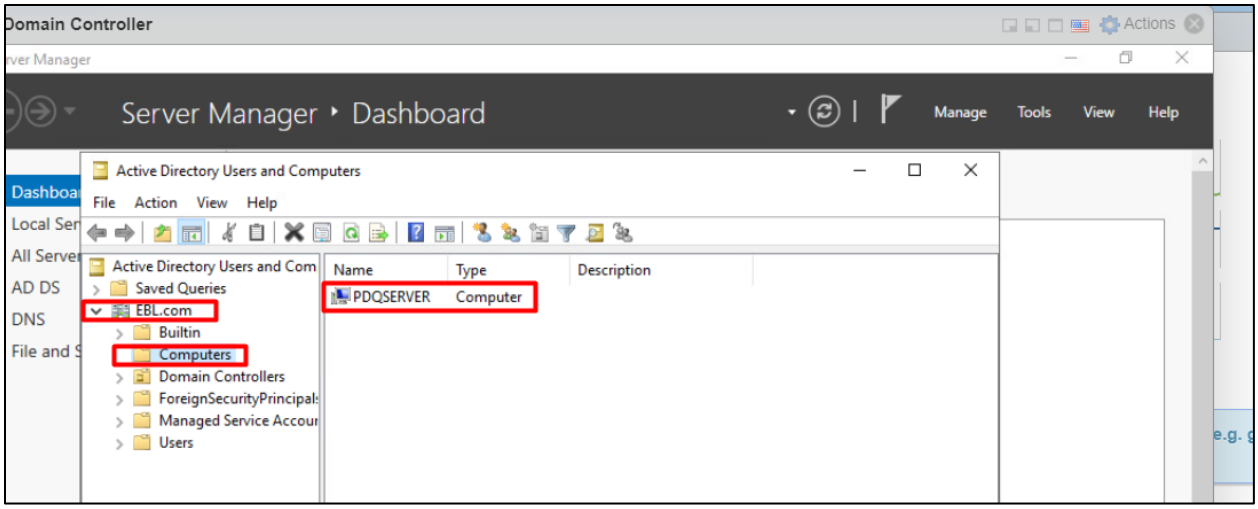


Figure 162 Internal web server added under EBL.com domain.

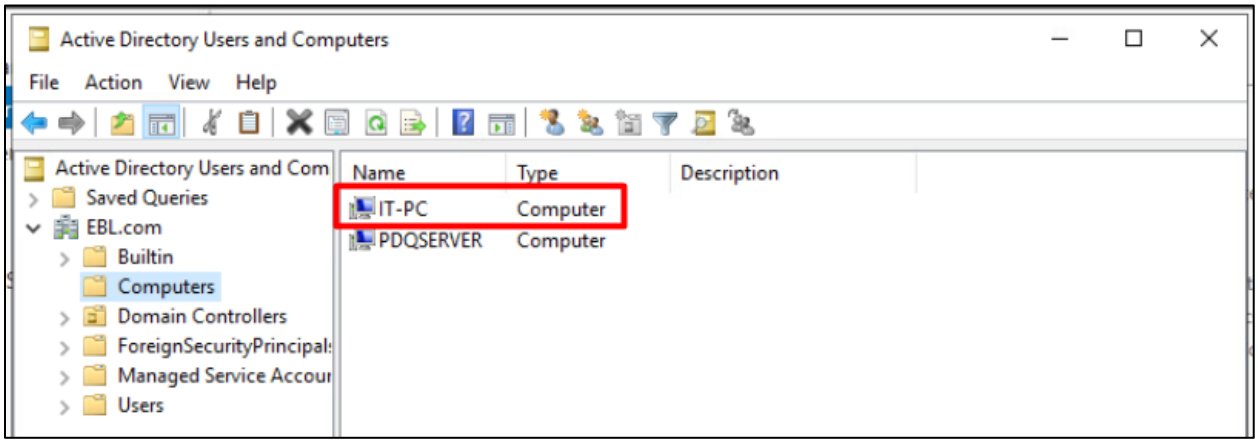


Figure 163 CL1 added under EBL.com domain.

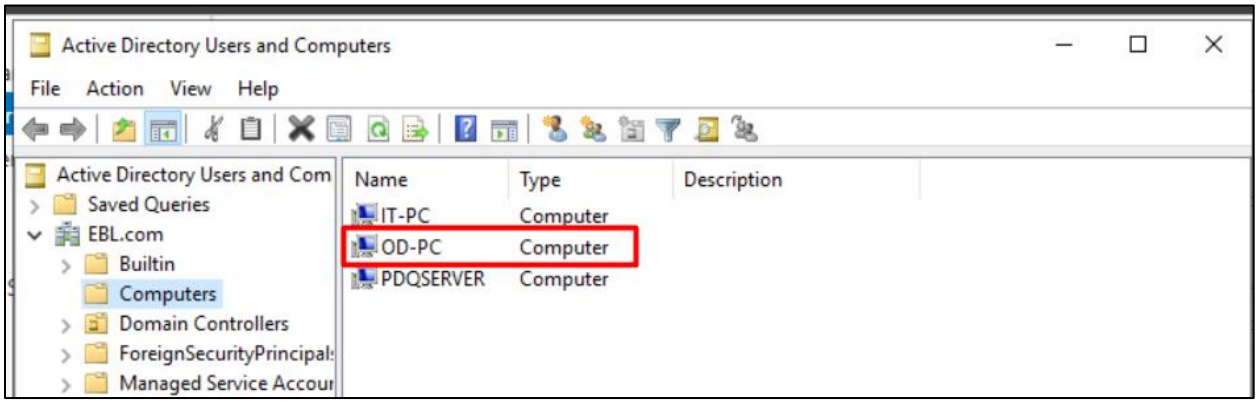


Figure 164 CL2 added under EBL.com domain.

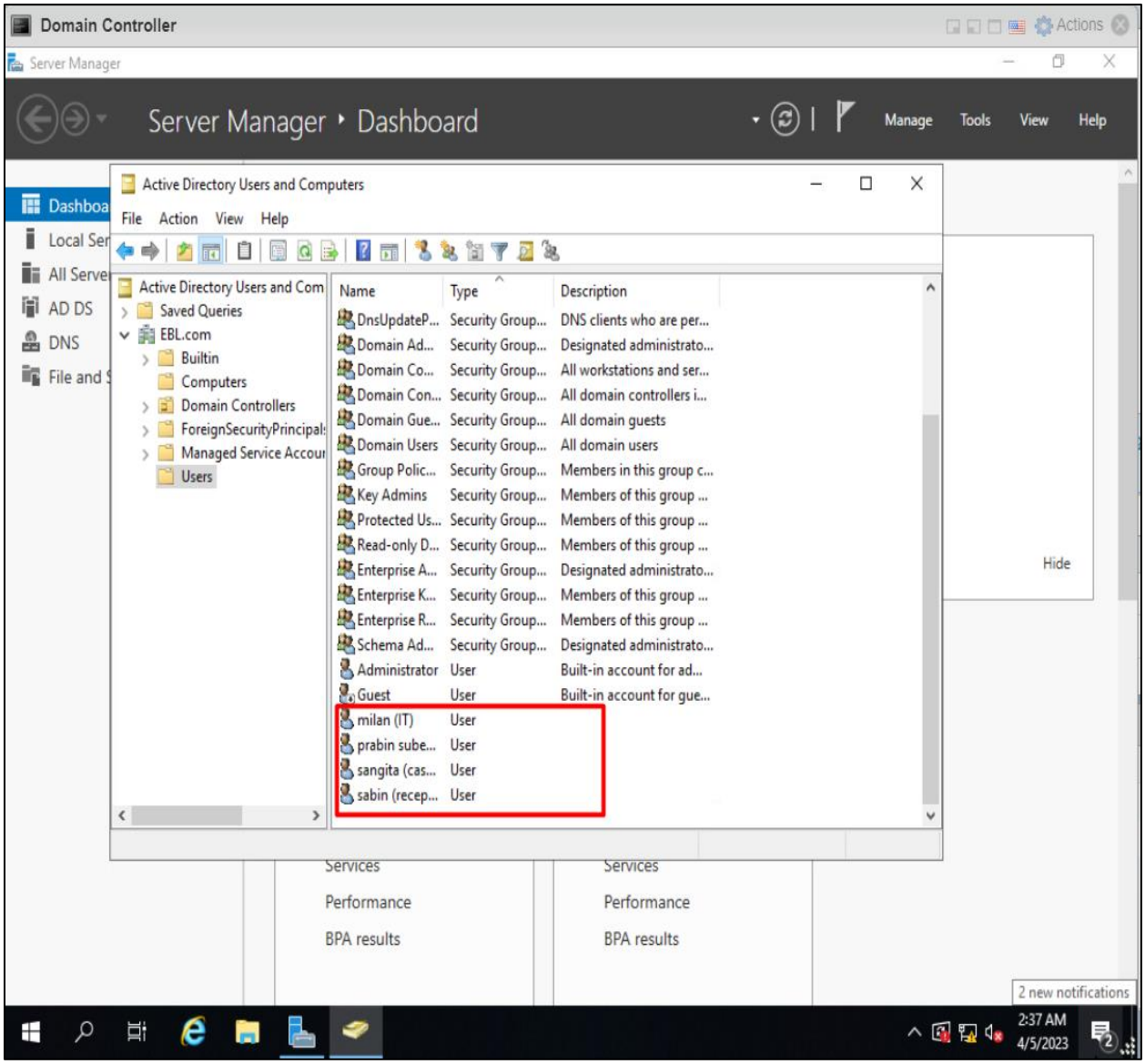


Figure 165 Users created for specific departments.

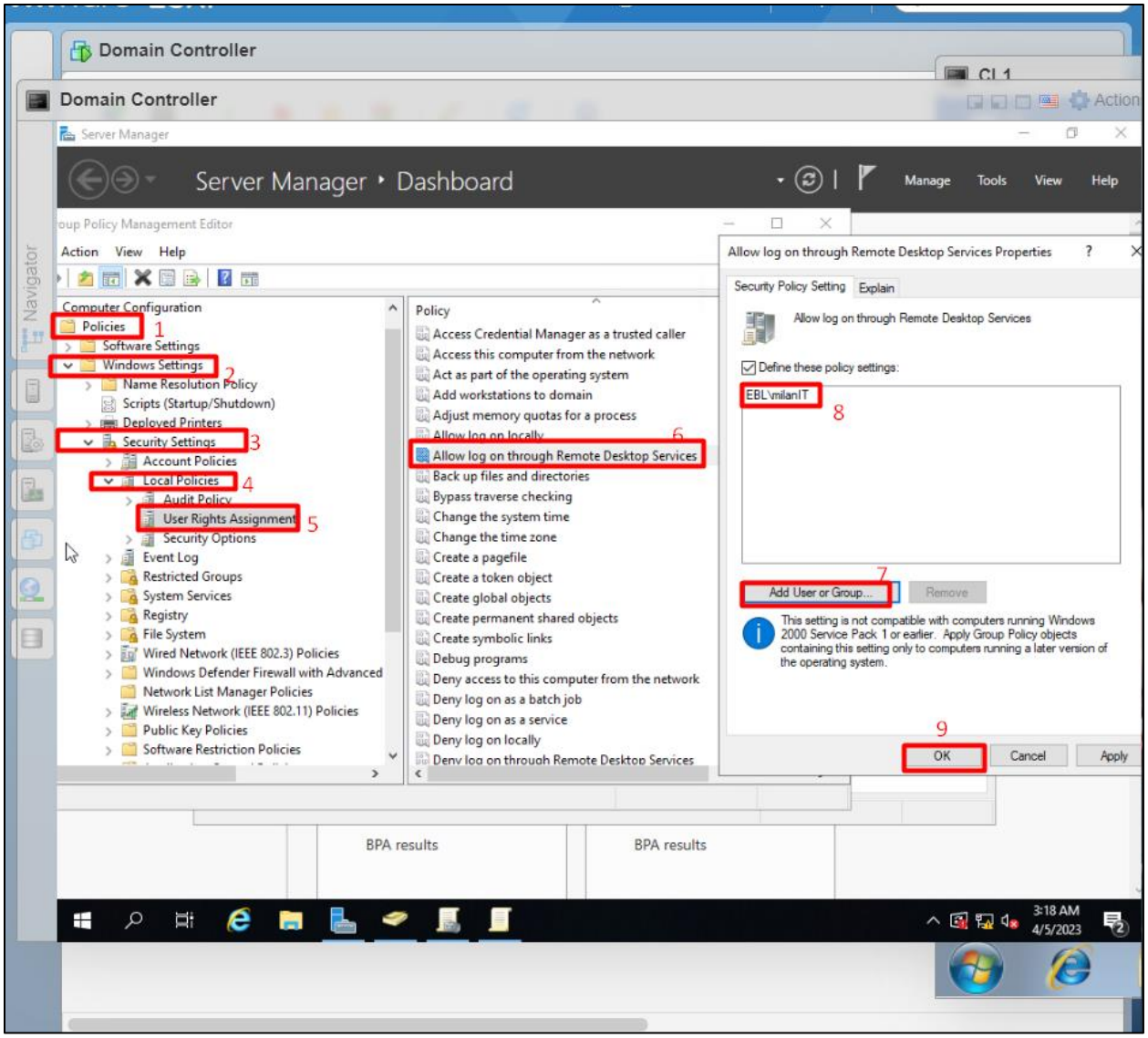


Figure 166 Editing policy to allow IT officers to remotely access domain controller.

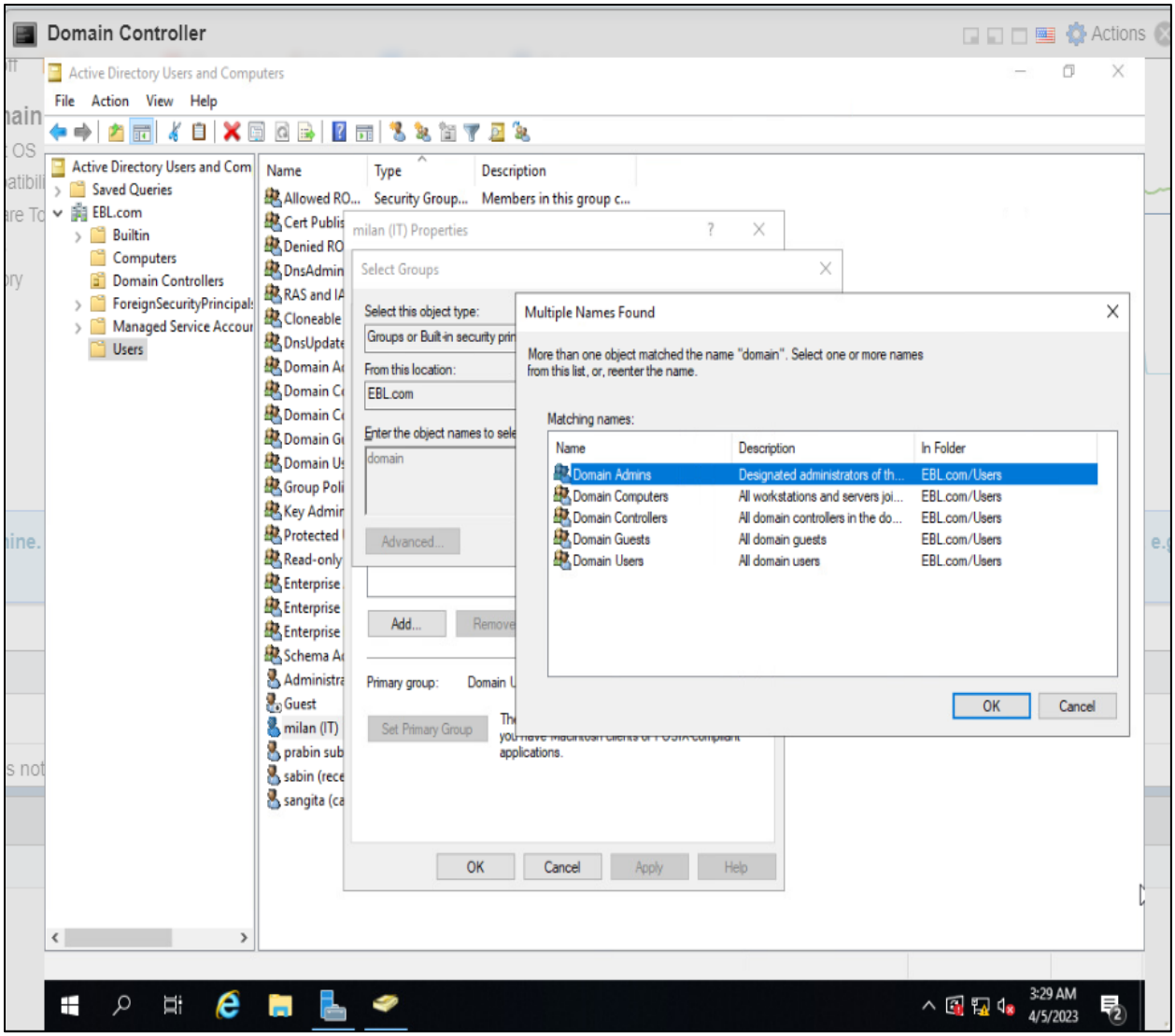


Figure 167 Providing admin privileges to IT officers.

8.4.4.3. Internal web server configuration

8.4.4.3.1. Creating website for internal users

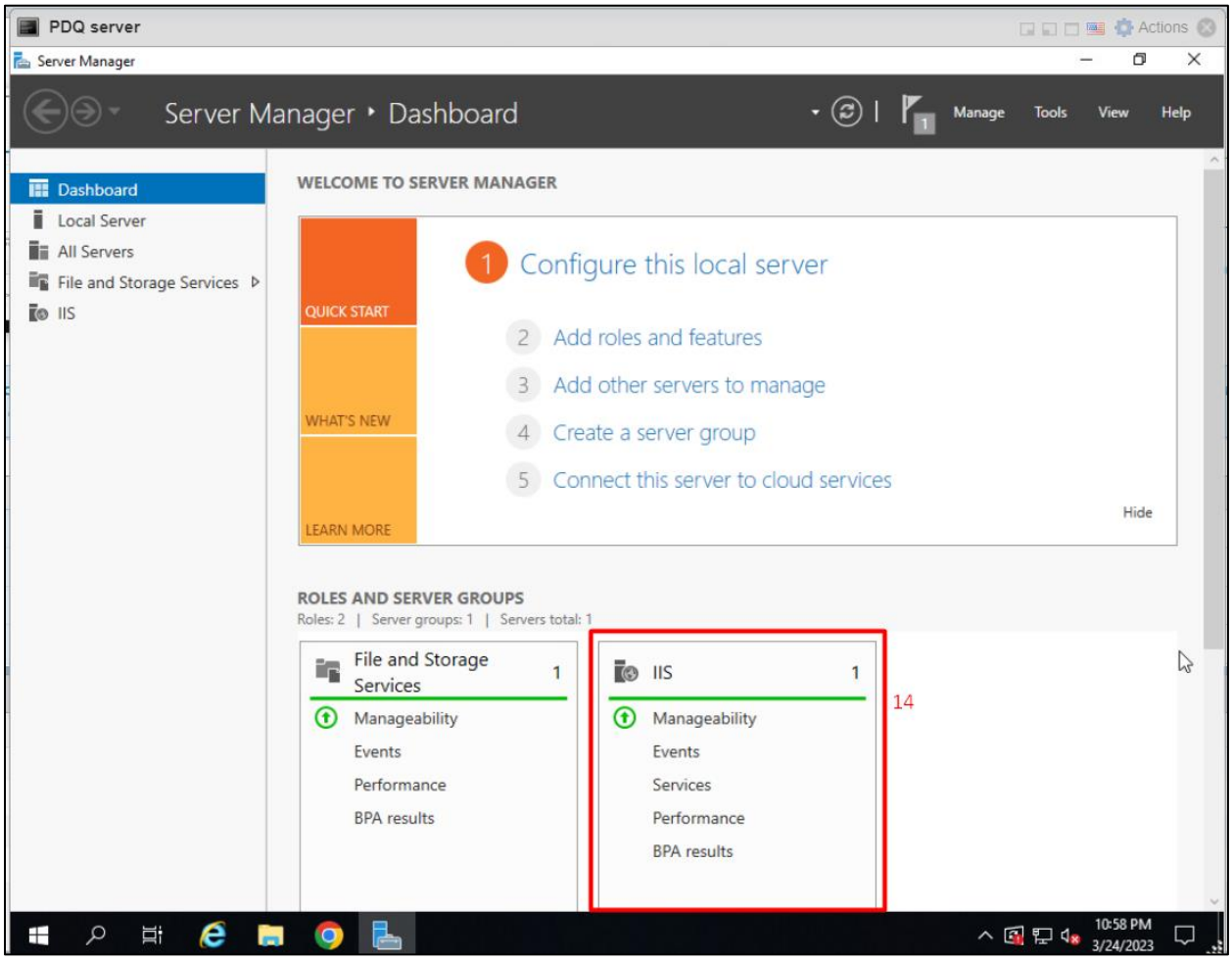


Figure 168 Web server role added successfully.

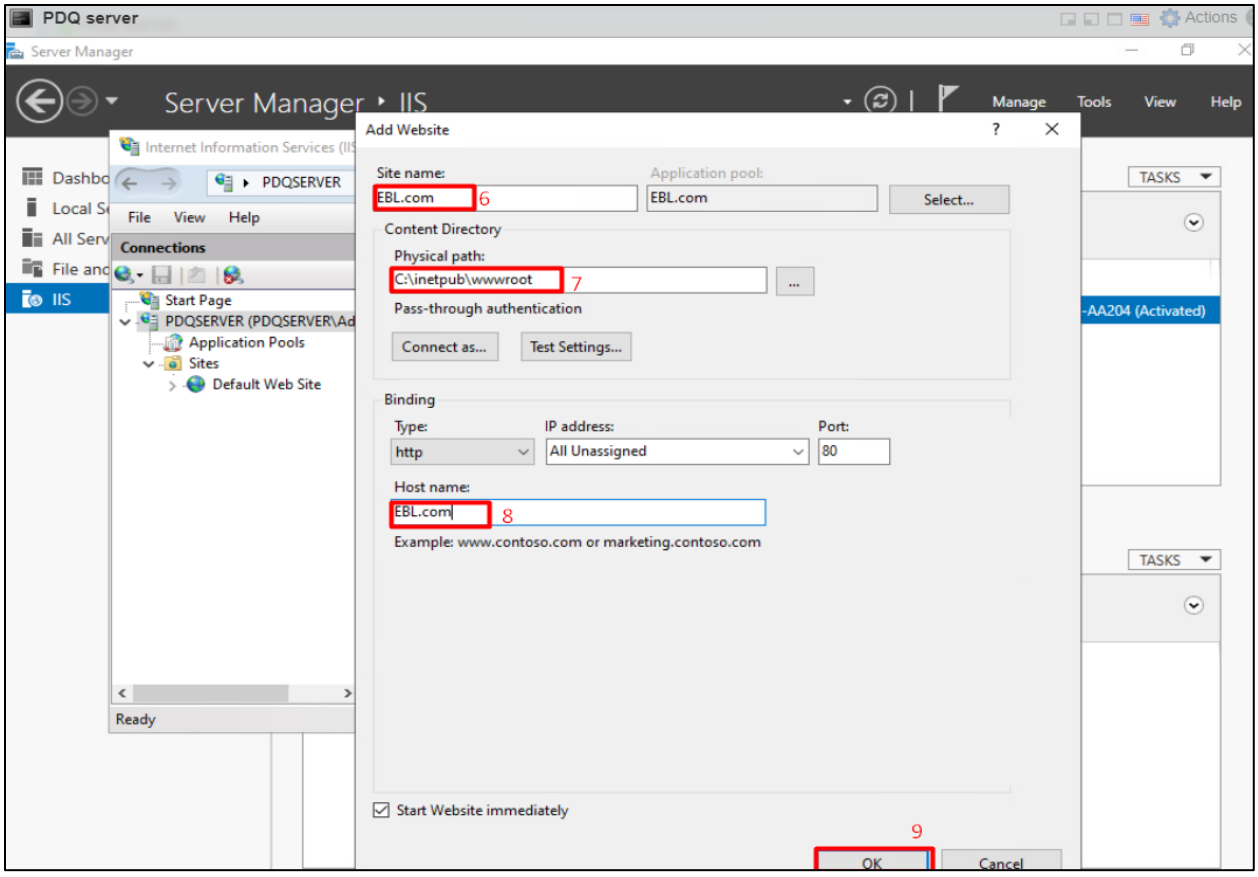


Figure 169 Creating internal website for internal users.

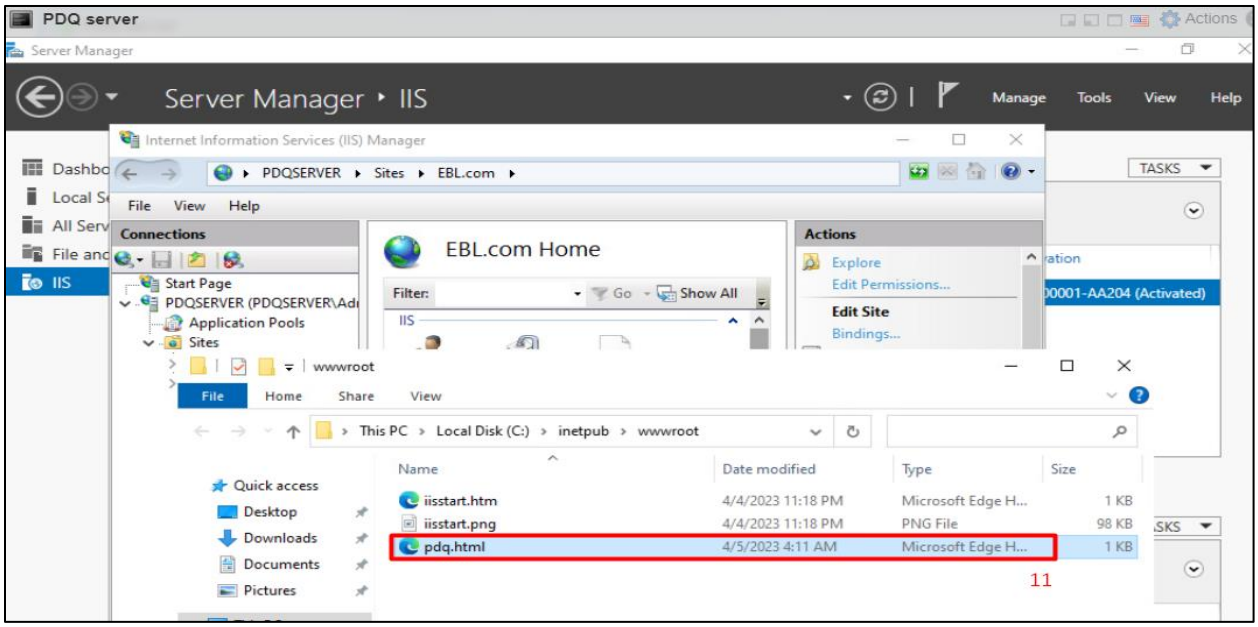


Figure 170 Creating simple html webpage.

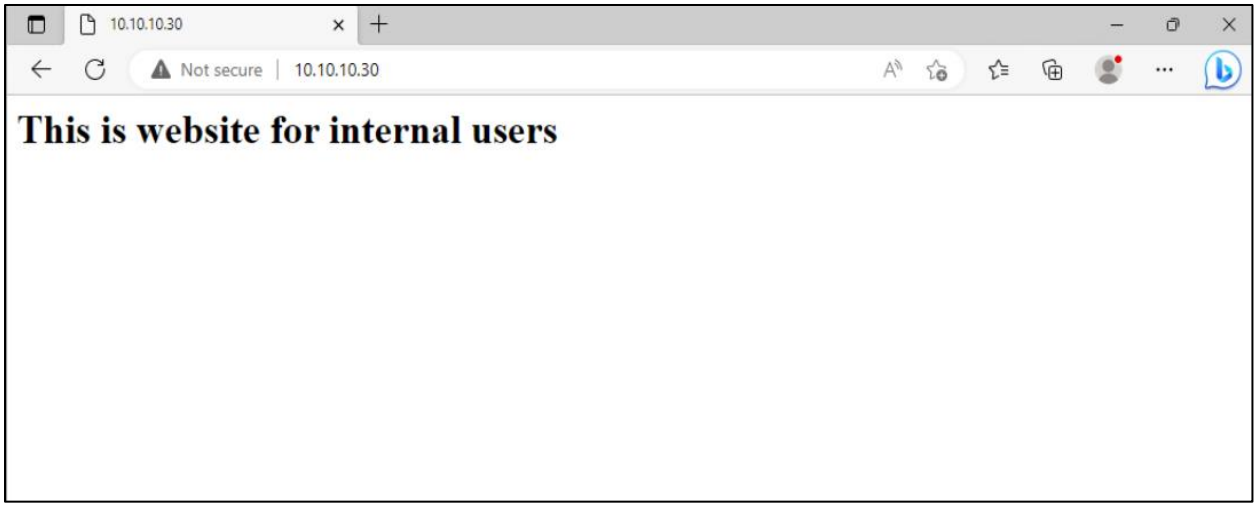


Figure 171 Accessing the hosted website.

8.4.4.3.2. Lansweeper configuration

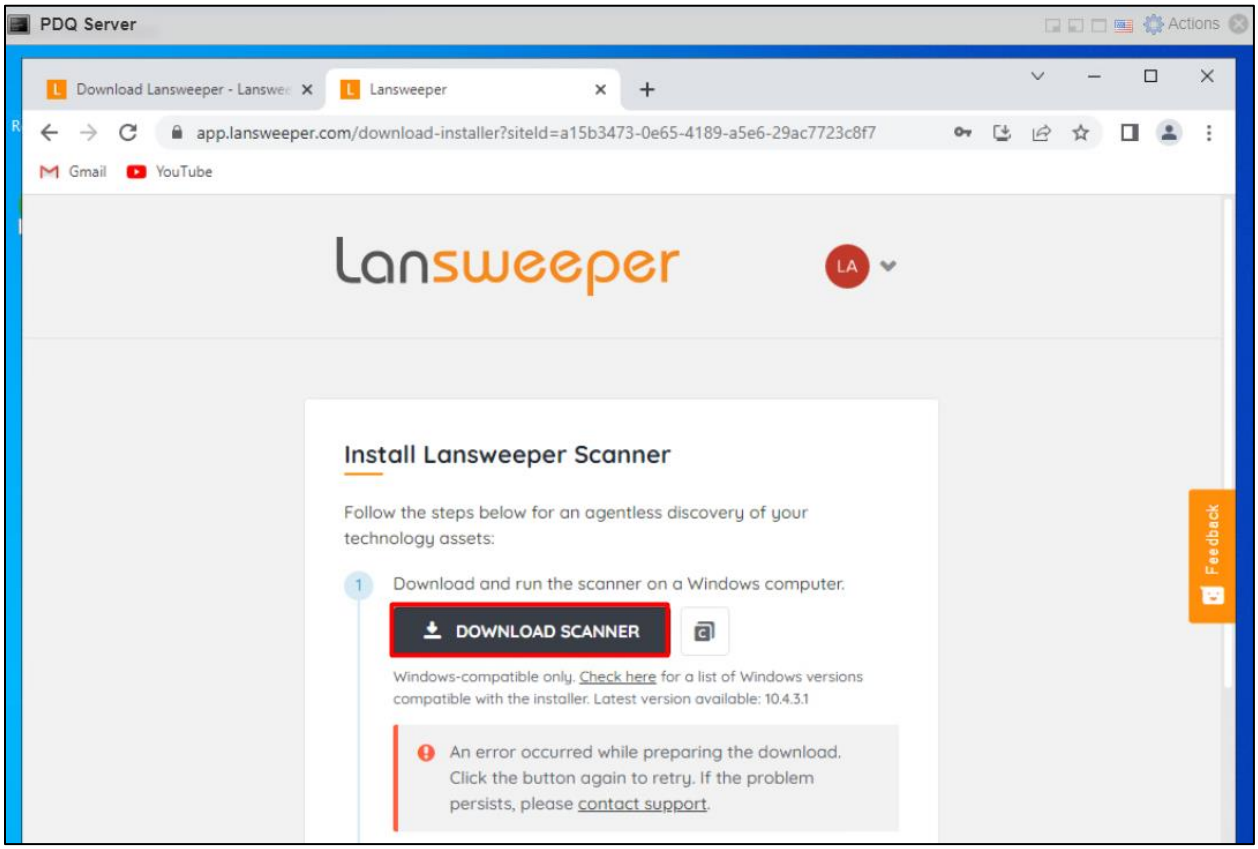


Figure 172 Downloading trial version of LAN sweeper.

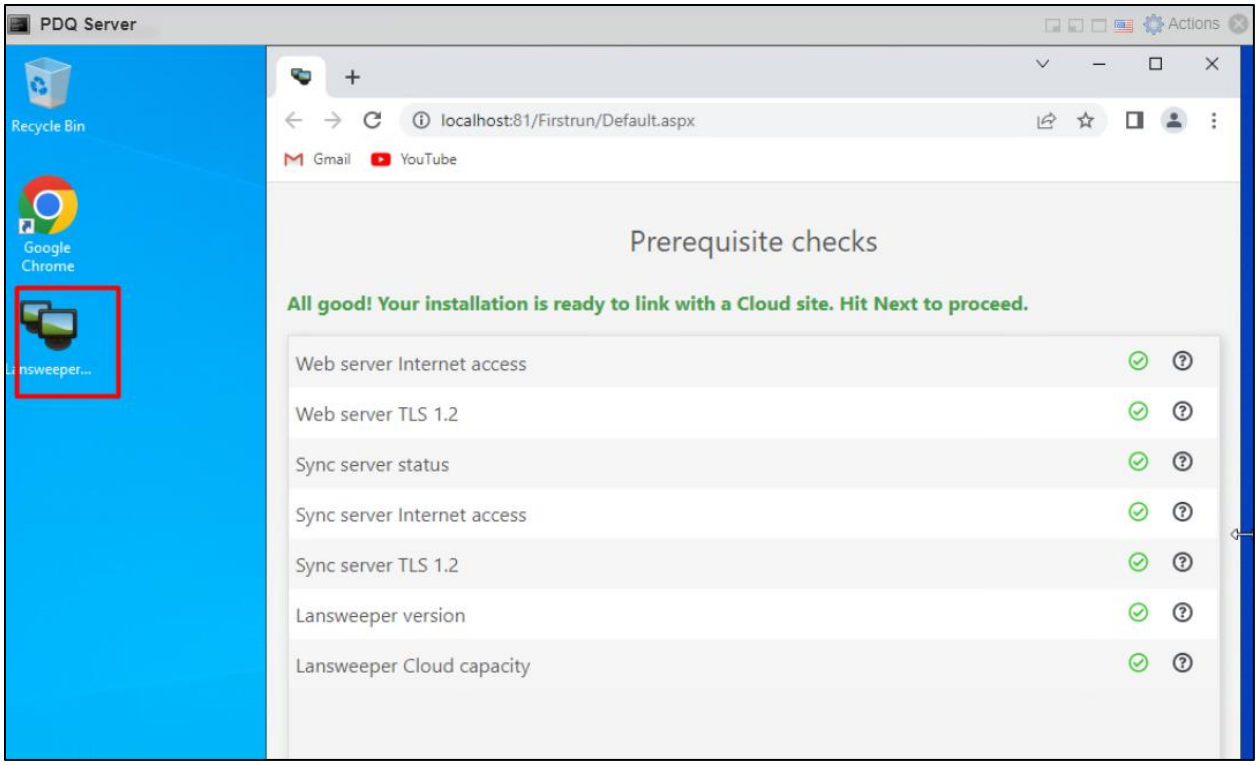


Figure 173 Checking the prerequisites status.

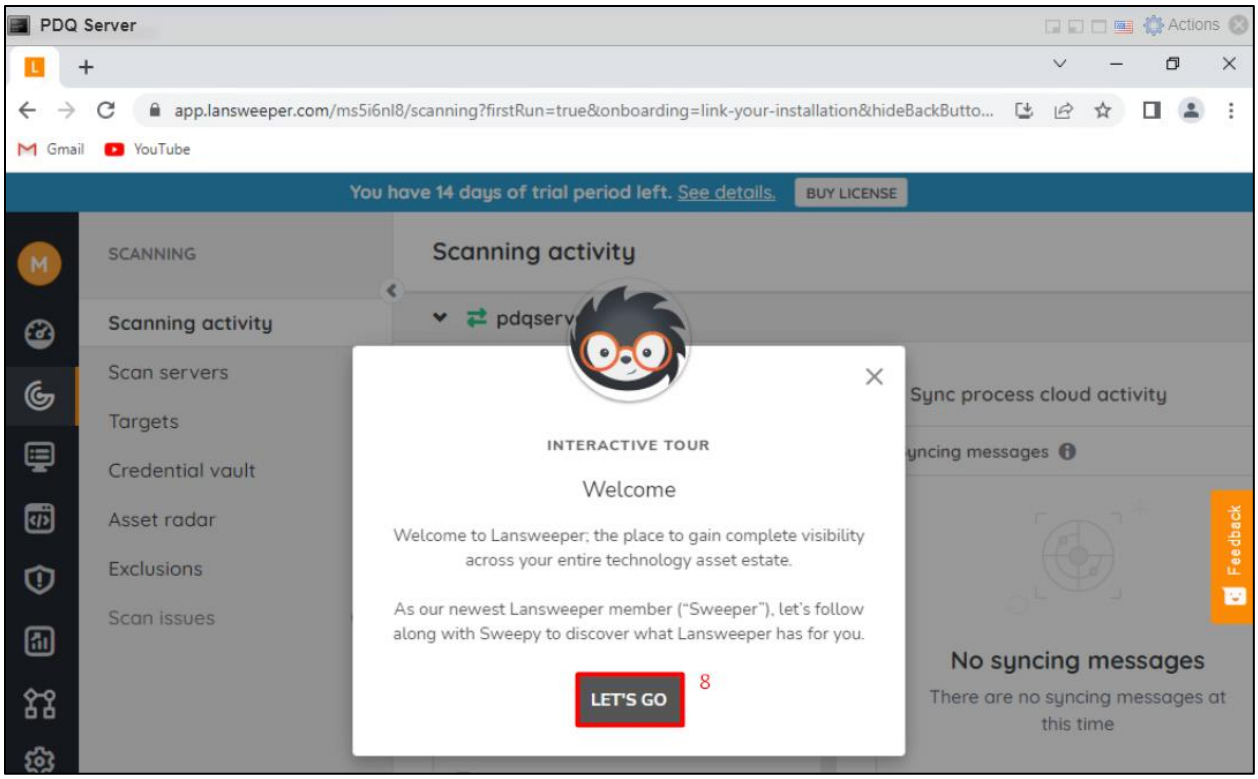


Figure 174 LAN sweeper installed successfully.

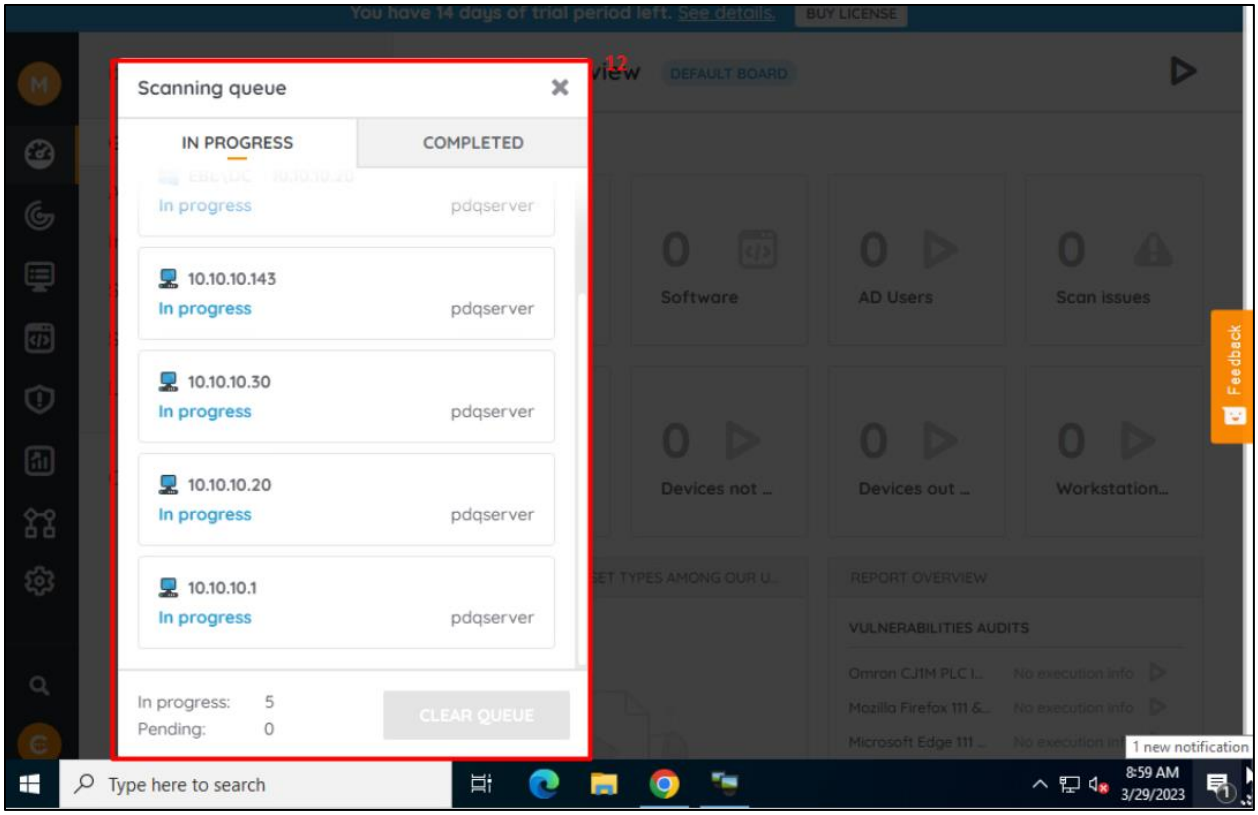


Figure 175 Started scanning assets.

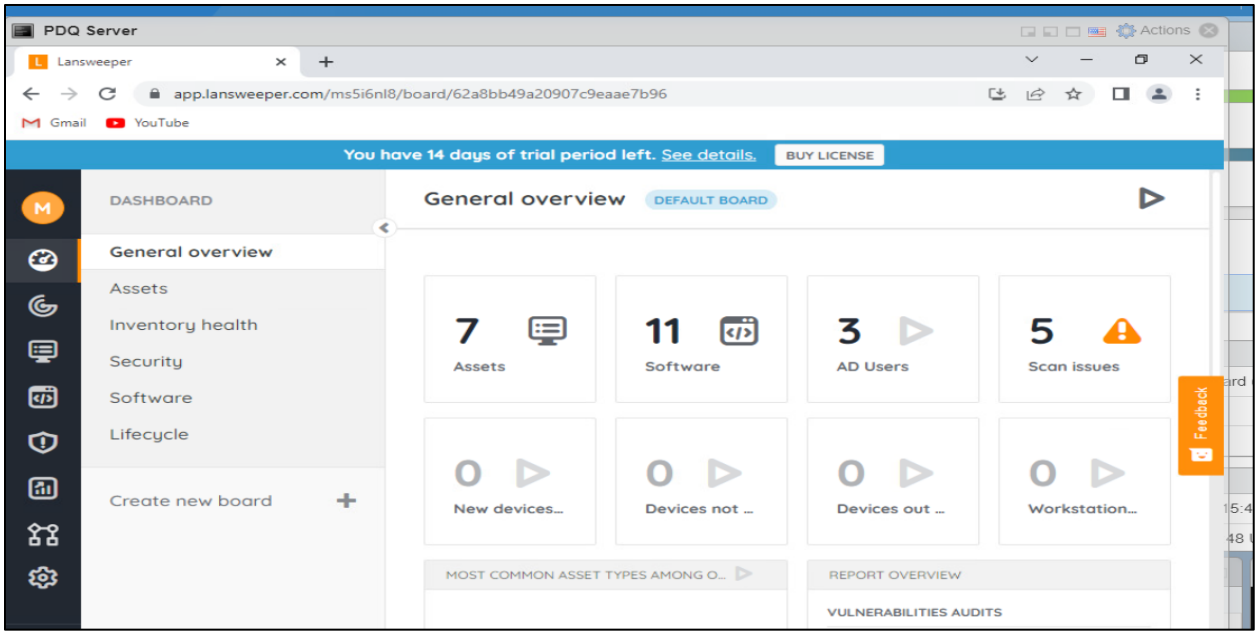


Figure 176 The scan results of LAN sweeper.

8.4.4.3.3. PDQ deploy configuration.

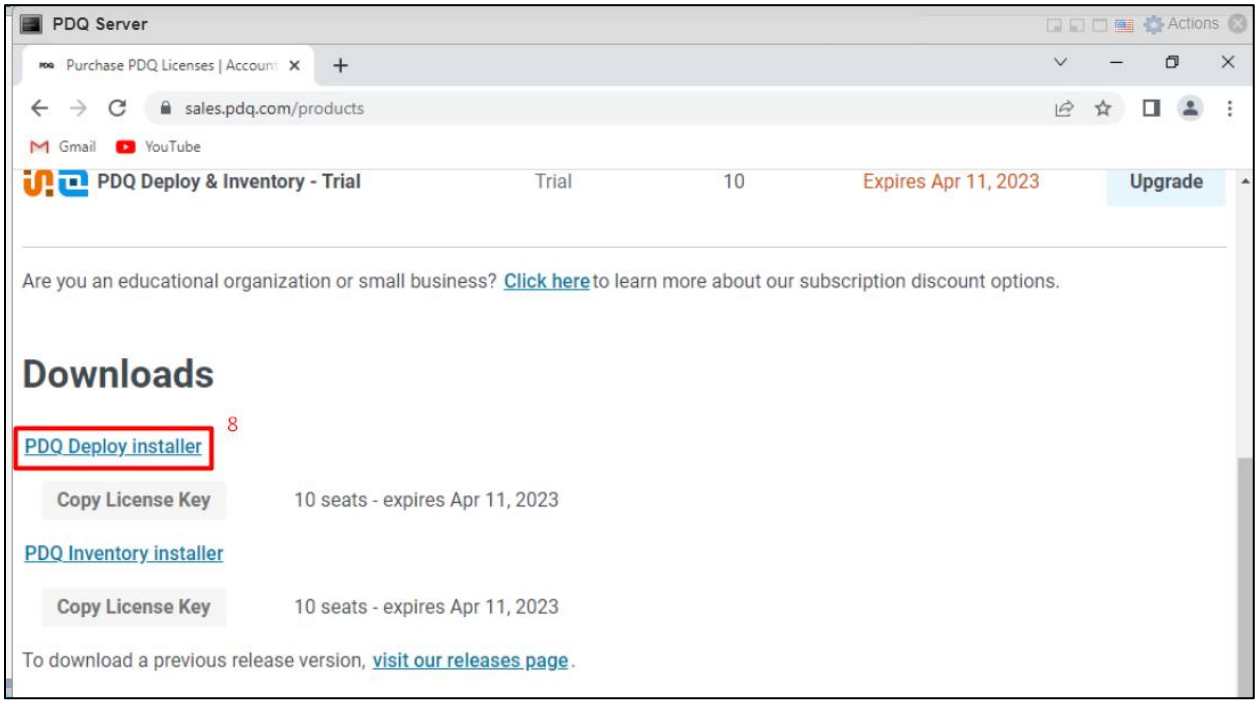


Figure 177 Installing trial version of PDQ deploy.

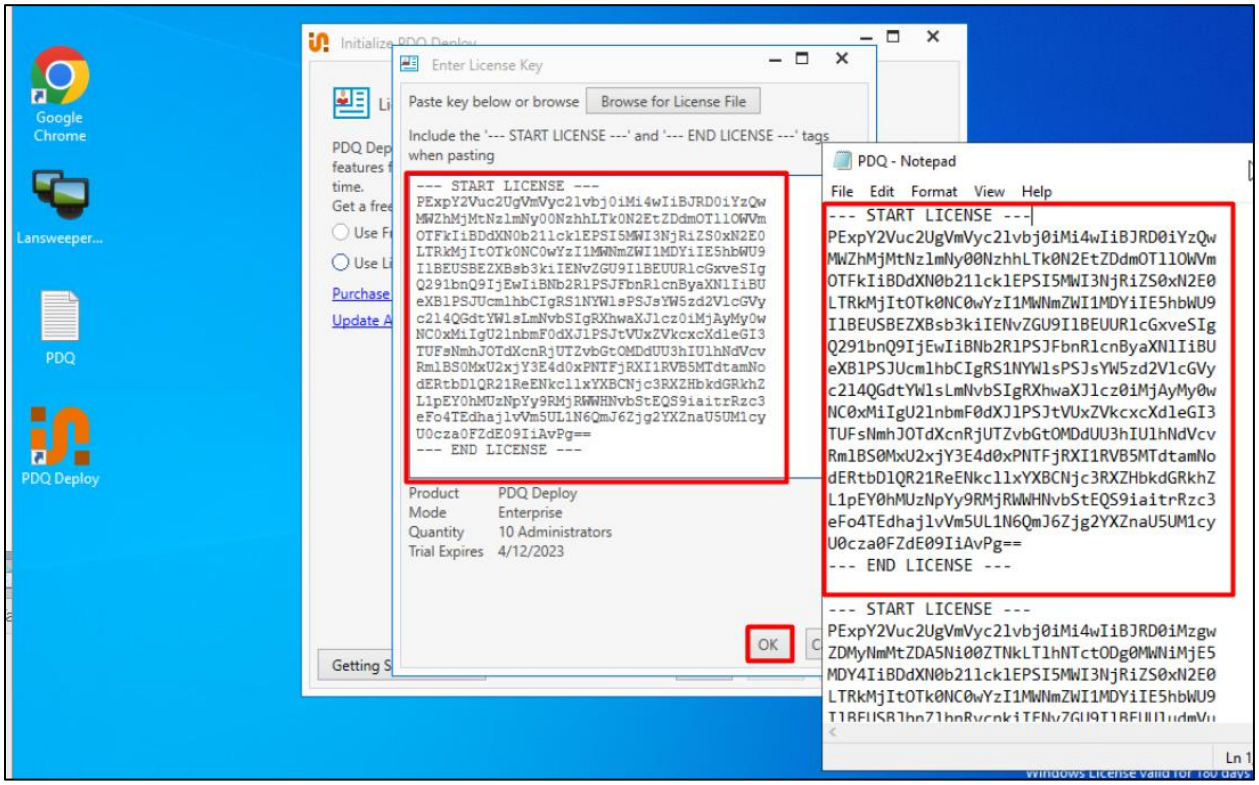


Figure 178 Enabling trial enterprise mode.

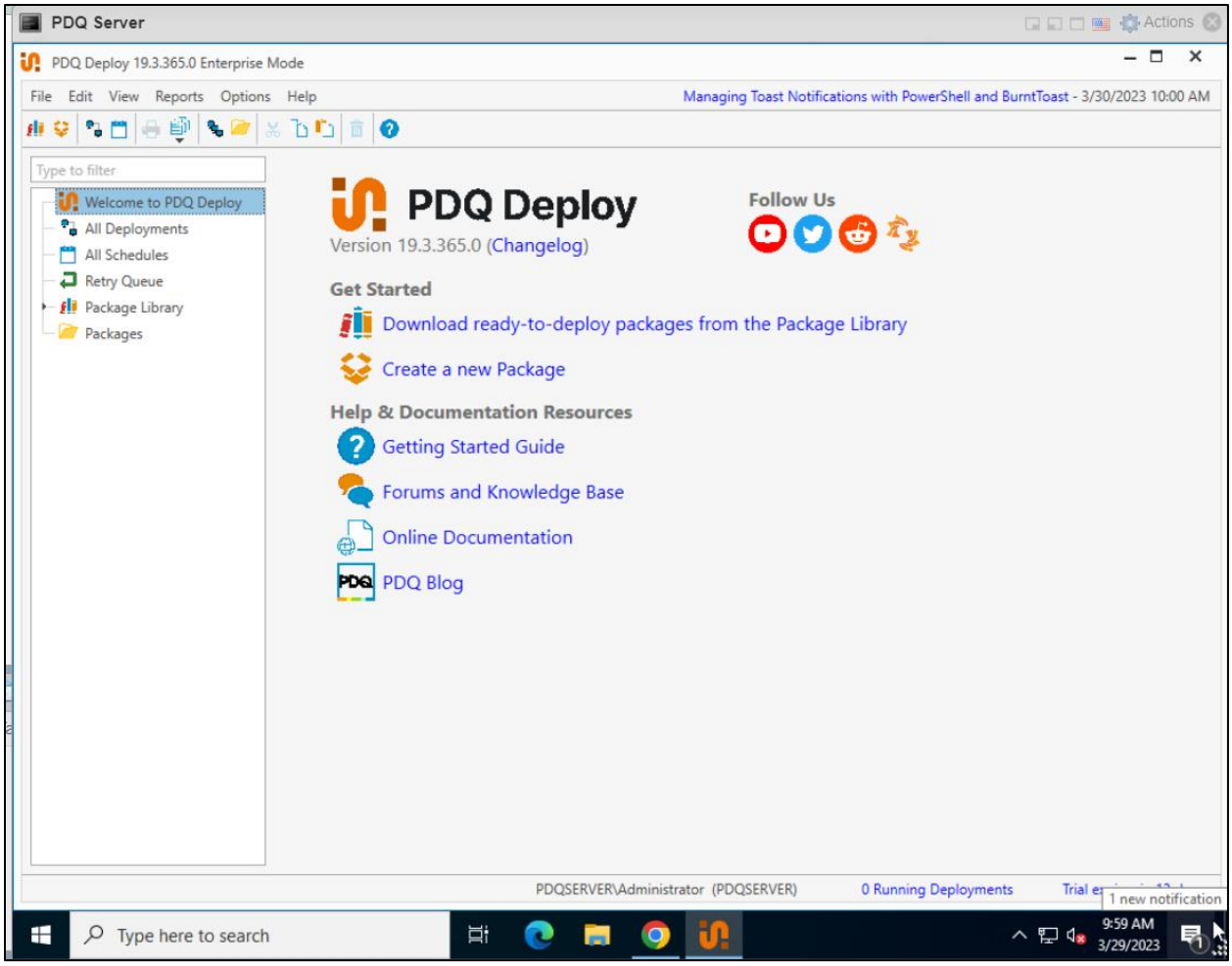


Figure 179 Successful PDQ deploy installation.

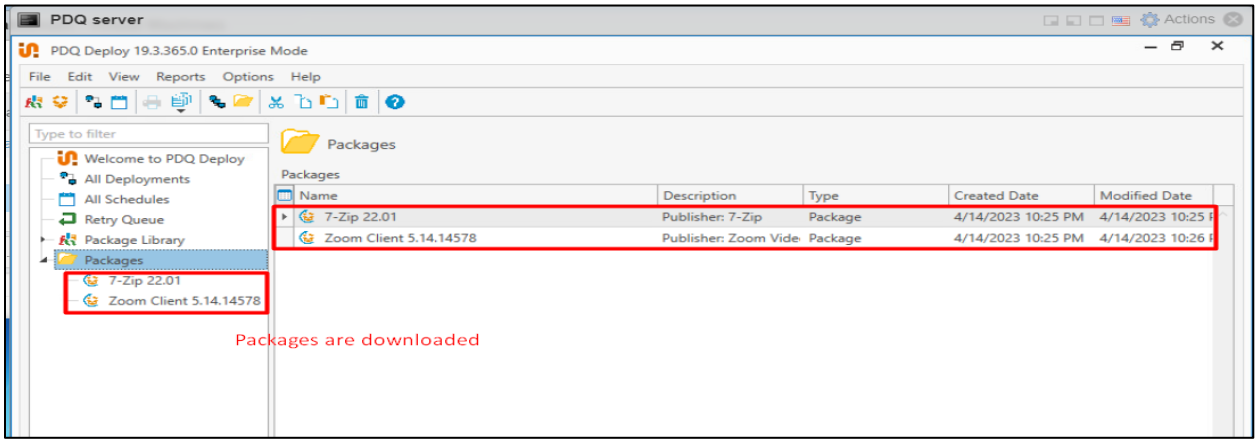


Figure 180 Downloaded packages for deployment.

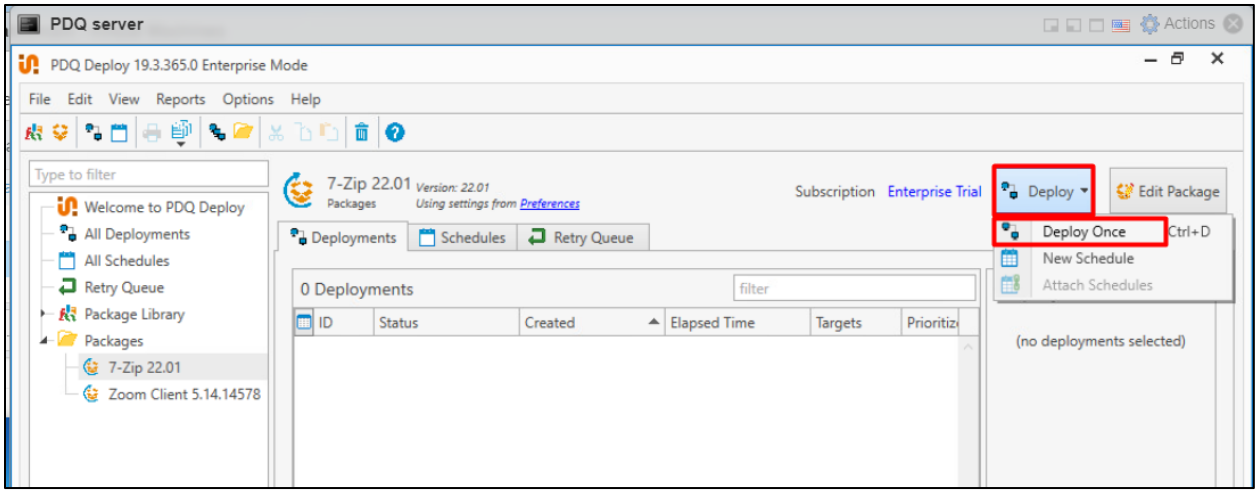


Figure 181 Manual package deployment (1)

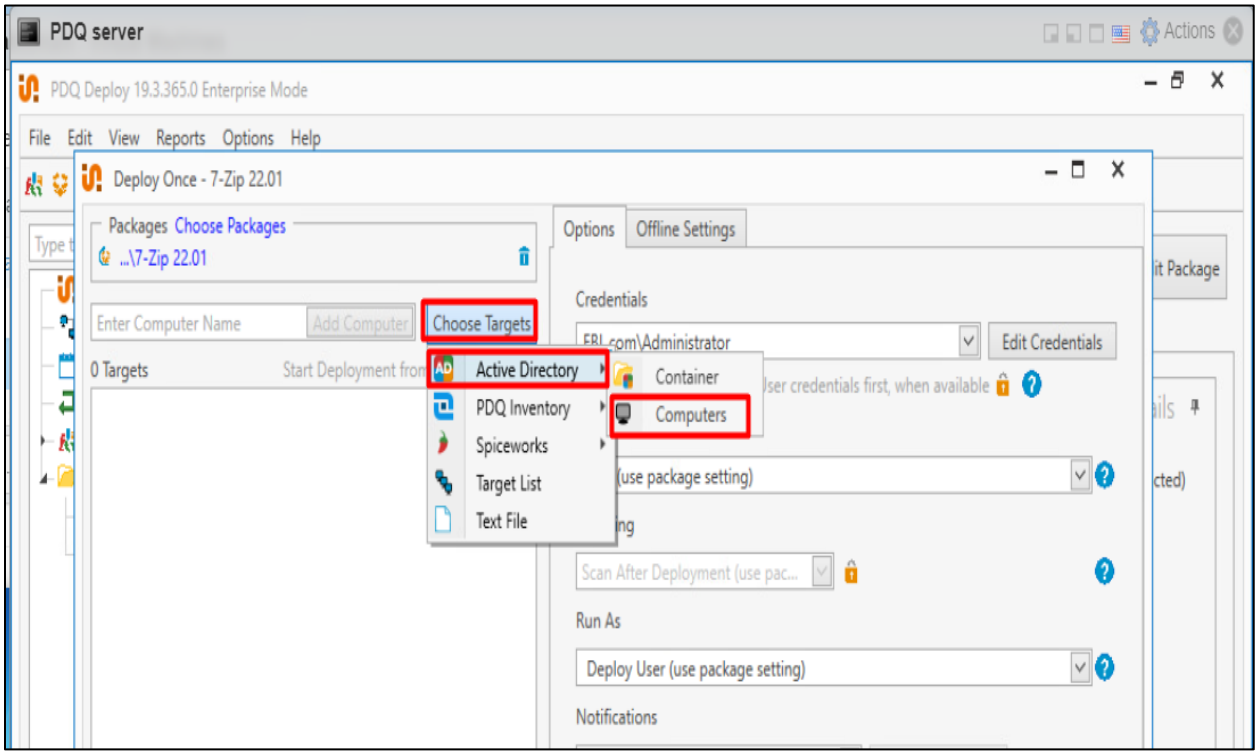


Figure 182 Selecting targets for deployment.

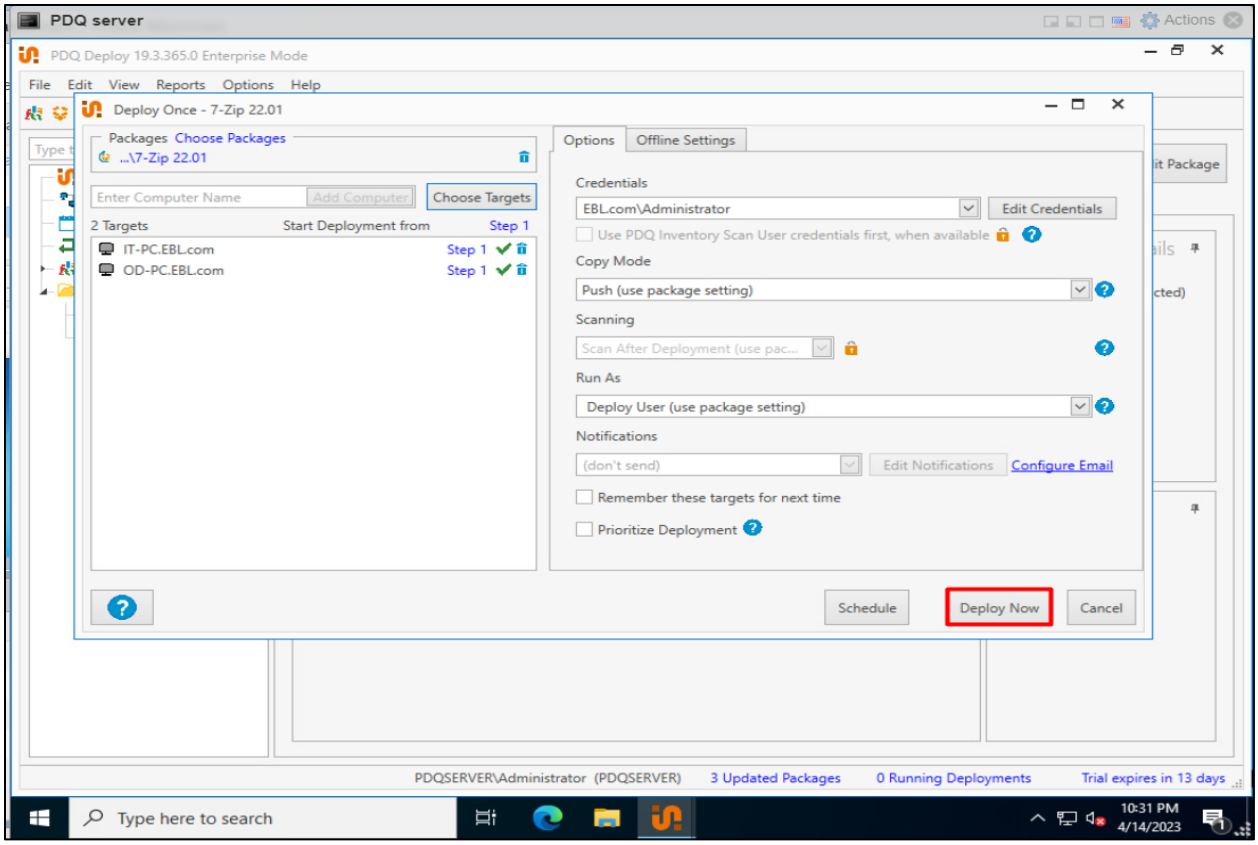


Figure 183 Started the deployment.

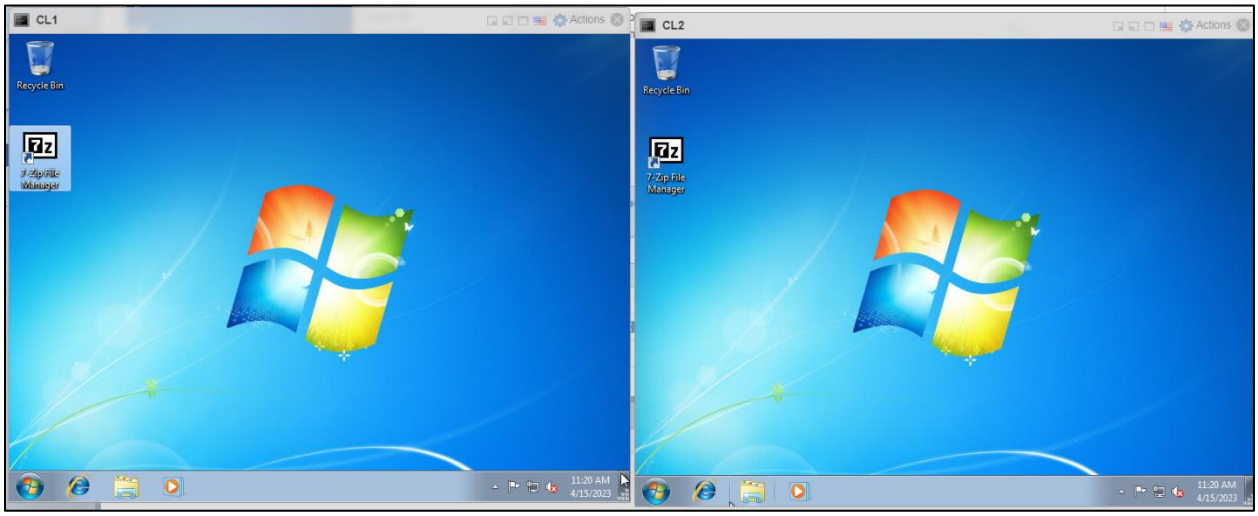


Figure 184 Package deployed successfully on targeted computers.

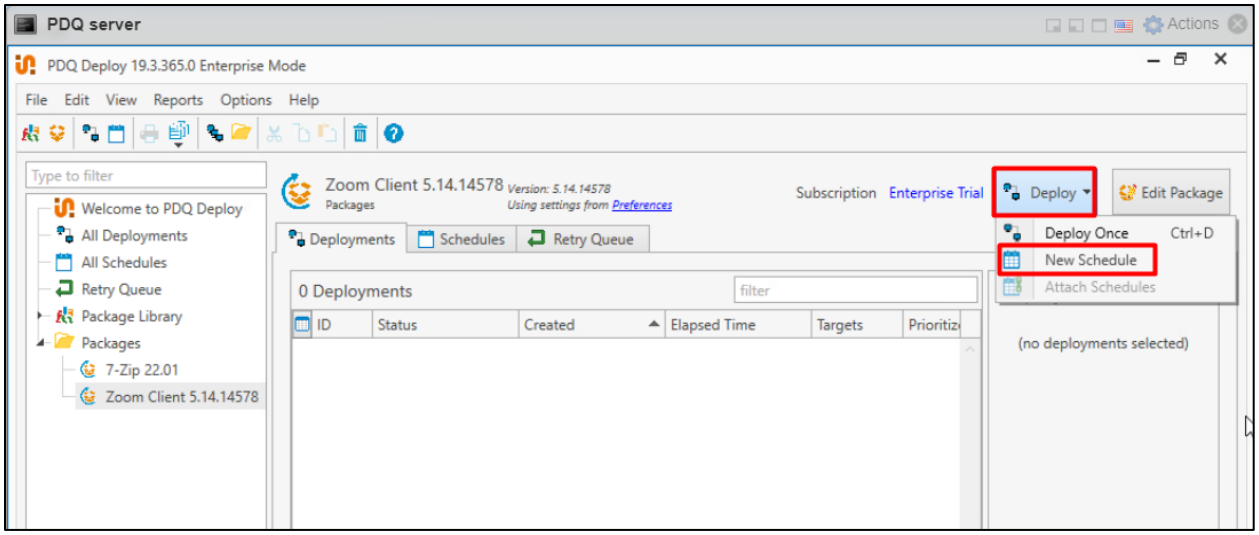


Figure 185 Creating scheduled package deployment.

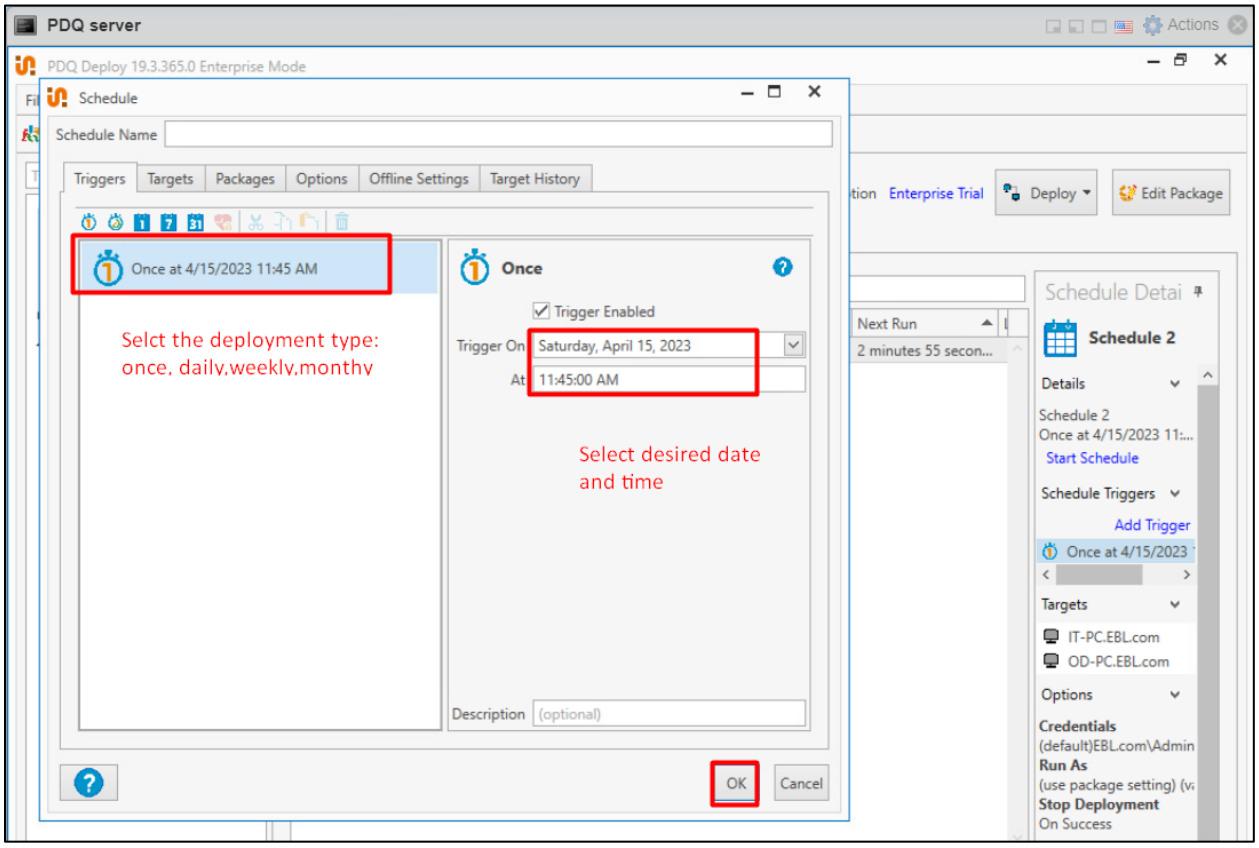


Figure 186 Selecting the deployment type, time, and date.

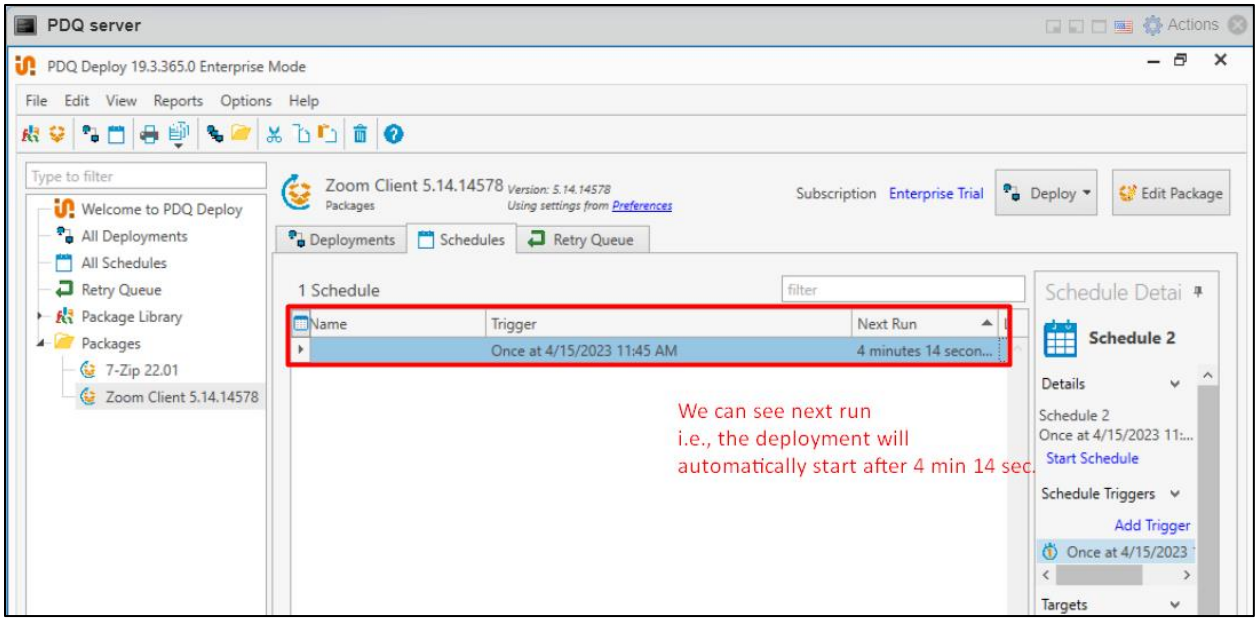


Figure 187 Package deployment count down started for deployment.

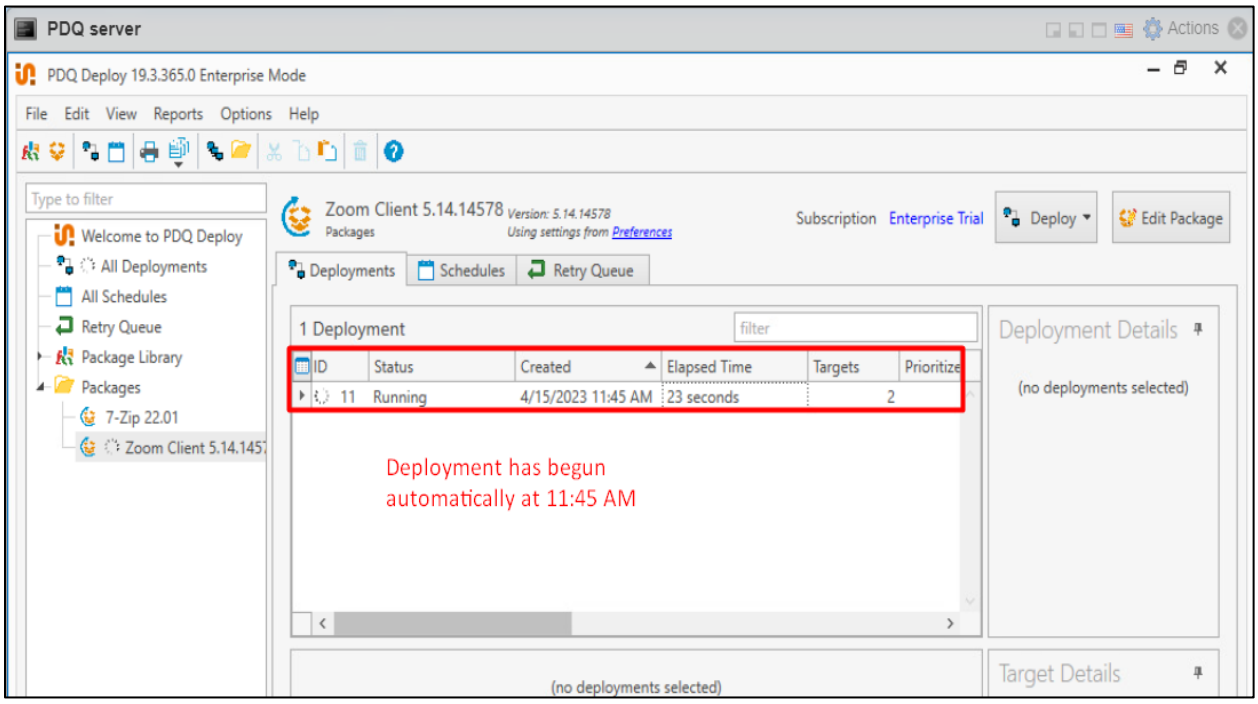


Figure 188 Package deployment started at scheduled time.

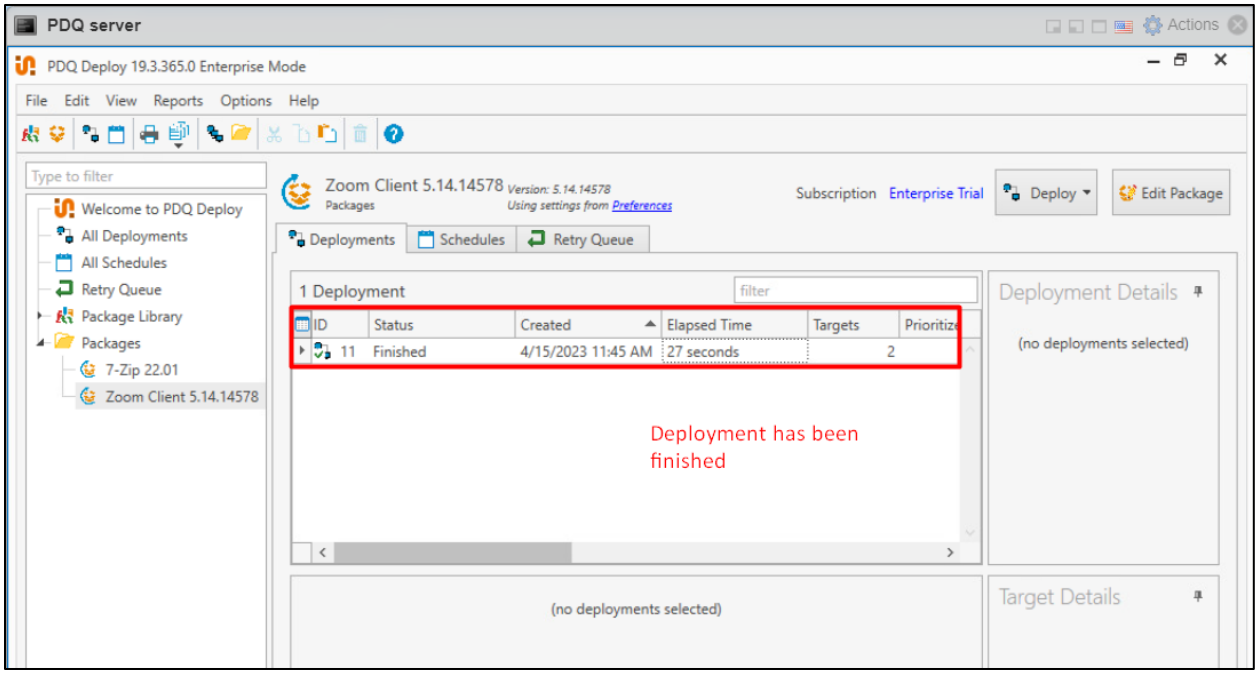


Figure 189 The deployment has been finished.

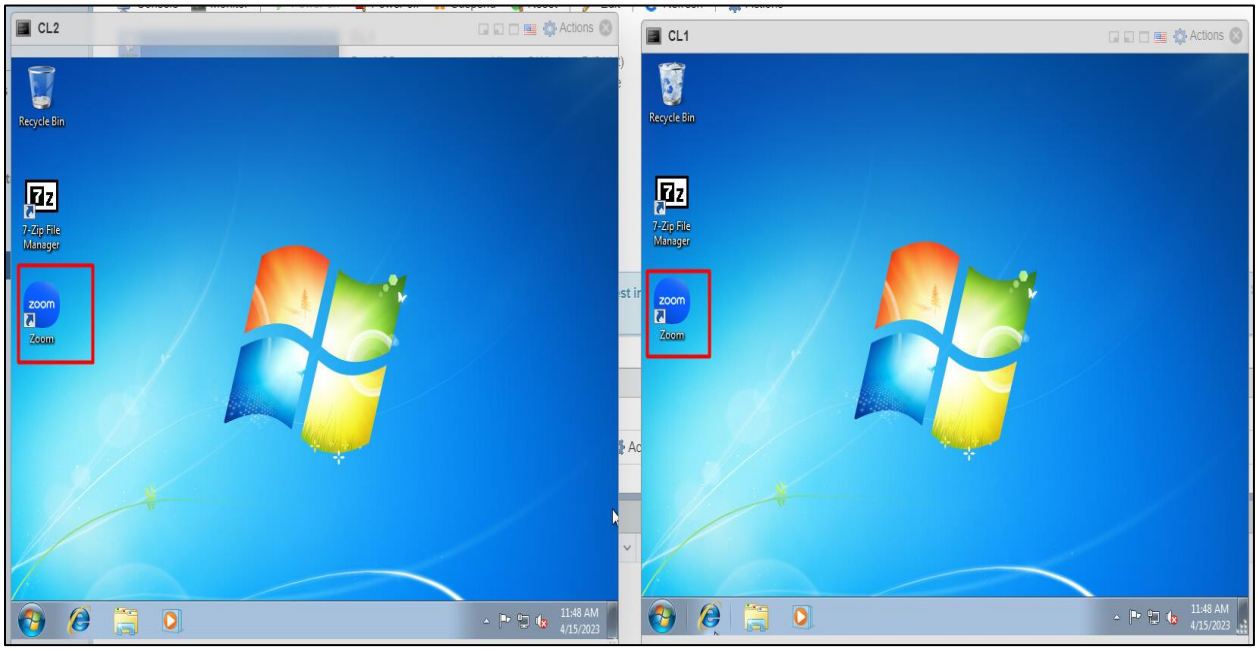


Figure 190 The package is successfully deployed in the targeted computers.

8.5. Appendix E: Designs

8.5.1. Work Breakdown structure

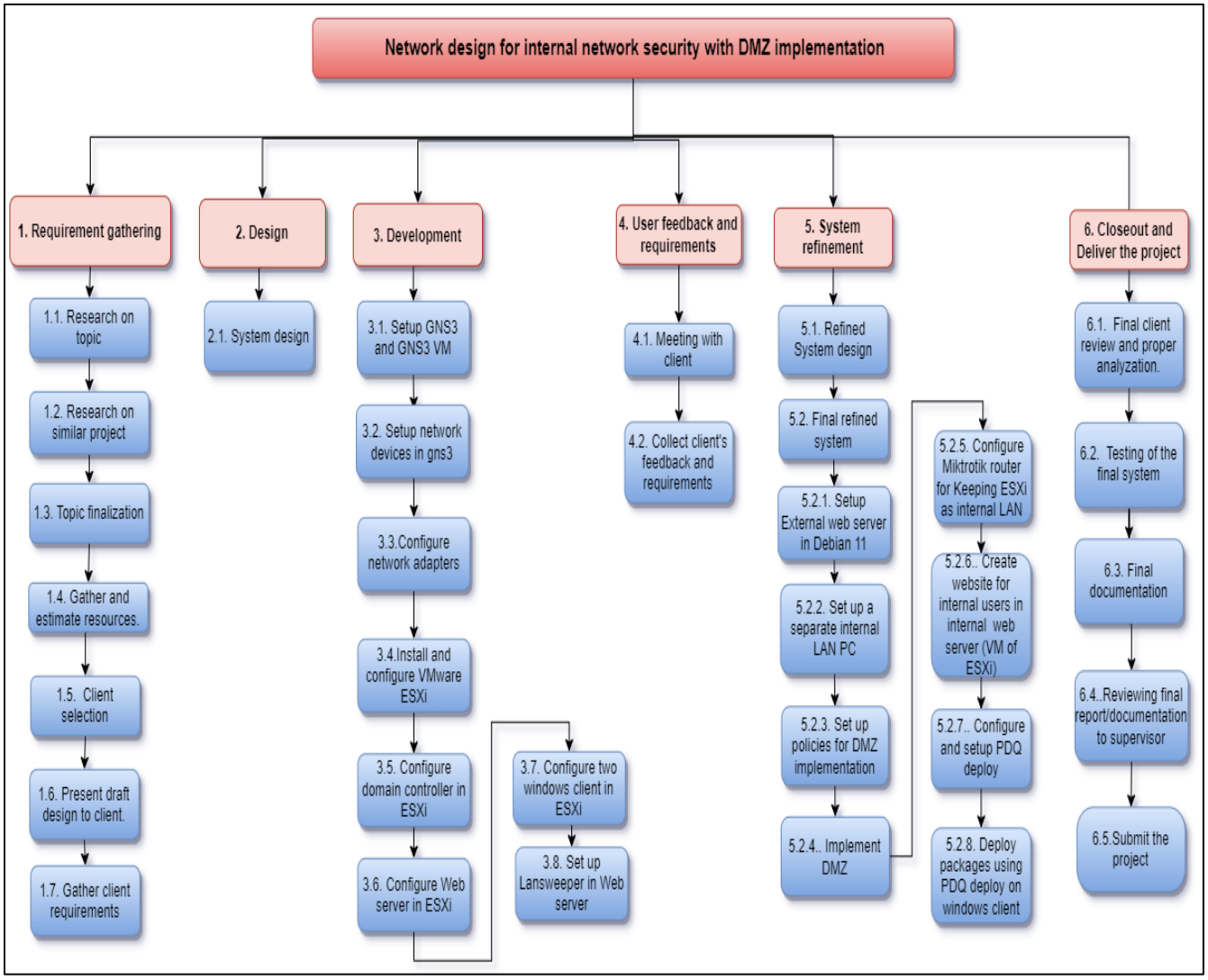


Figure 191 Work breakdown structure.

8.5.2. Gantt Chart

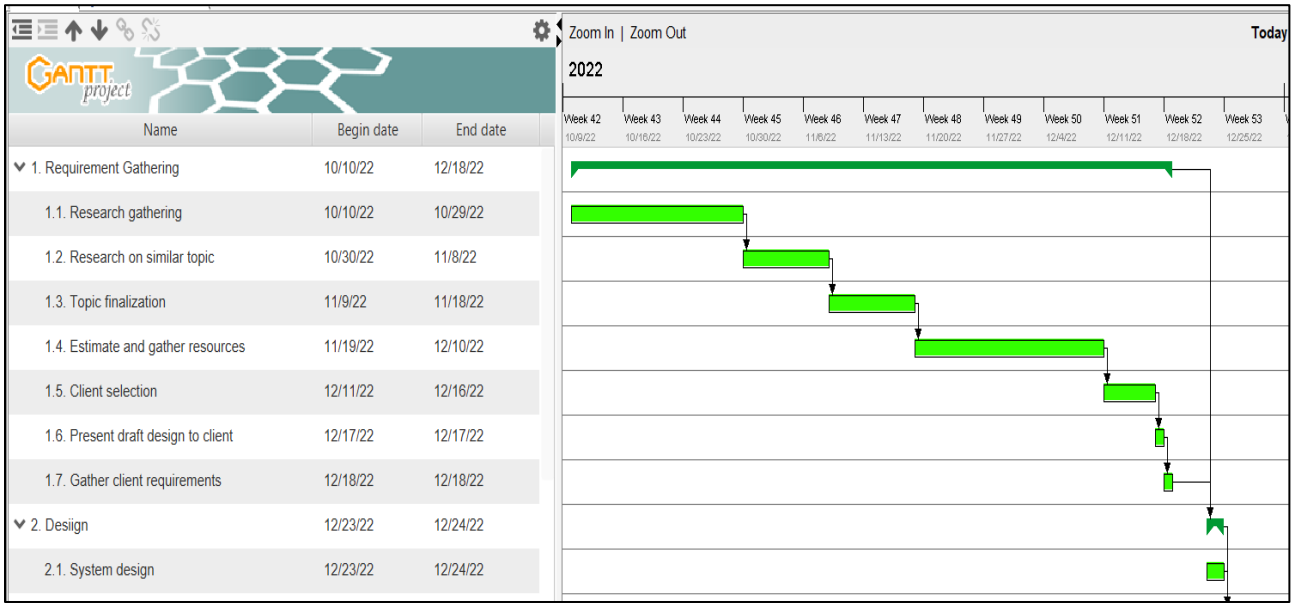


Figure 192 Gantt chart (1).

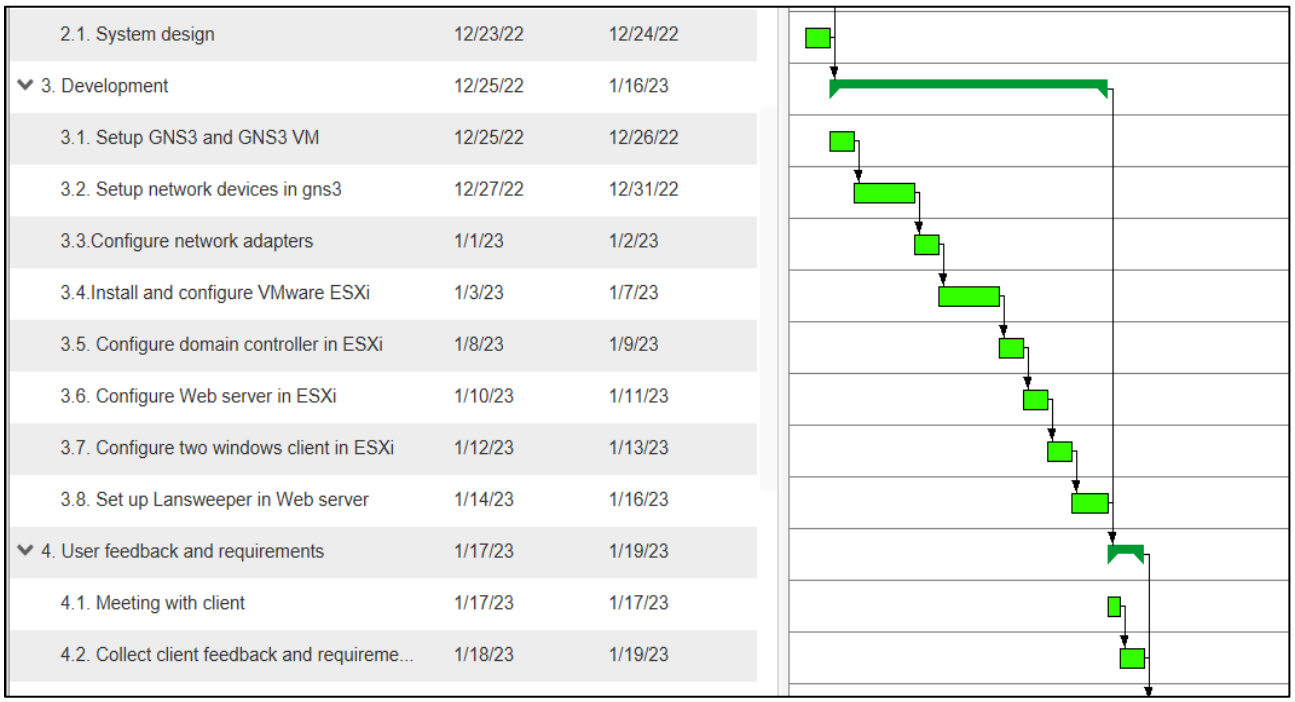


Figure 193 Gantt chart (2).

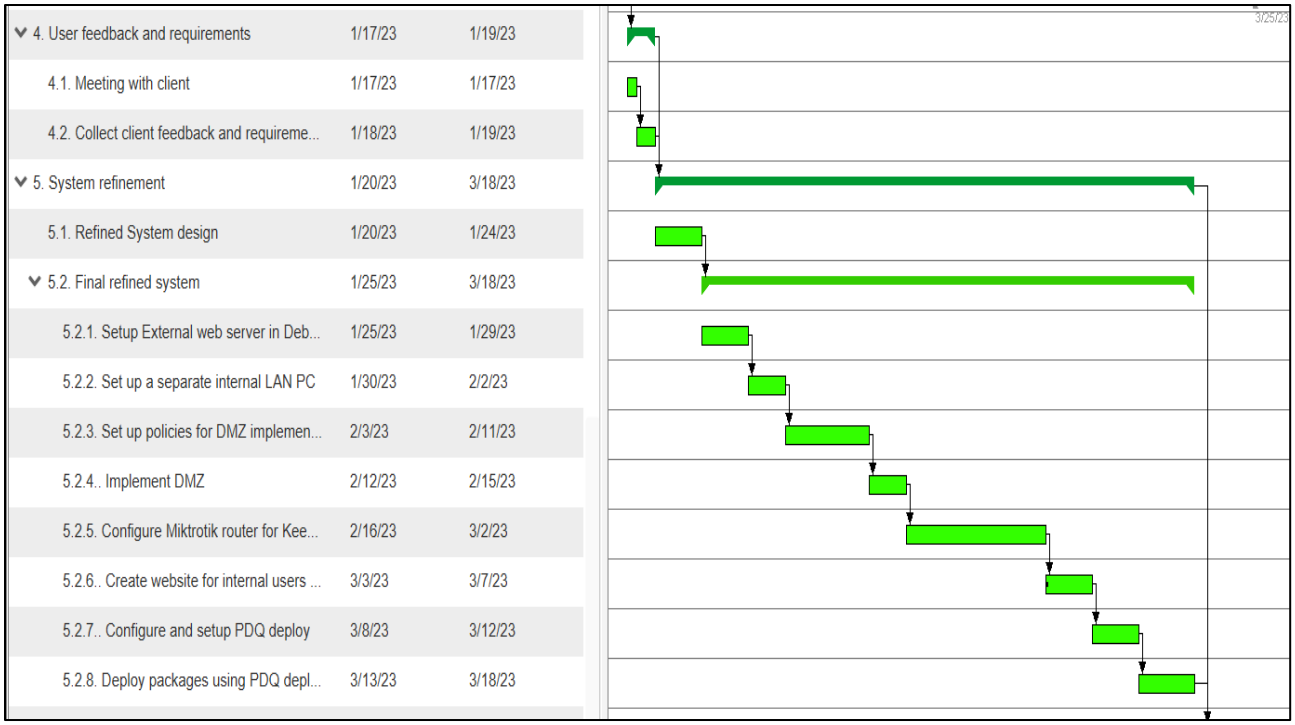


Figure 194 Gantt chart (3).

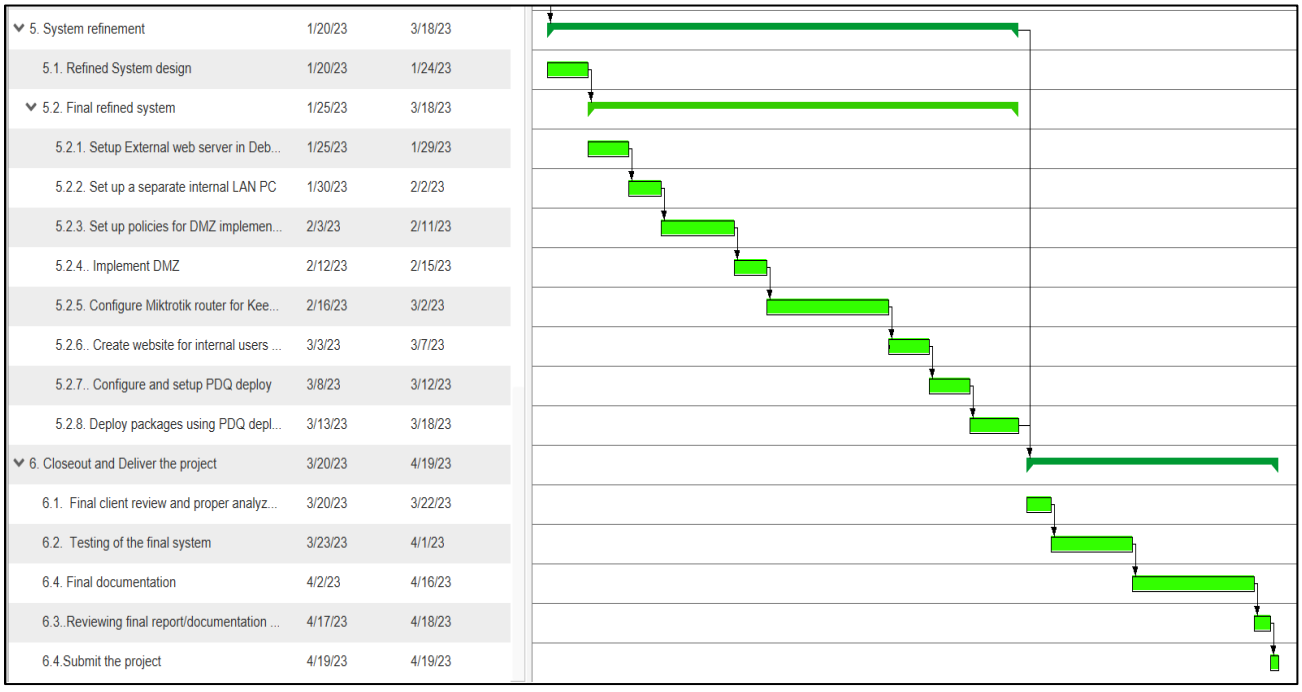


Figure 195 Gantt chart (4).

8.5.3. Draft proposal design

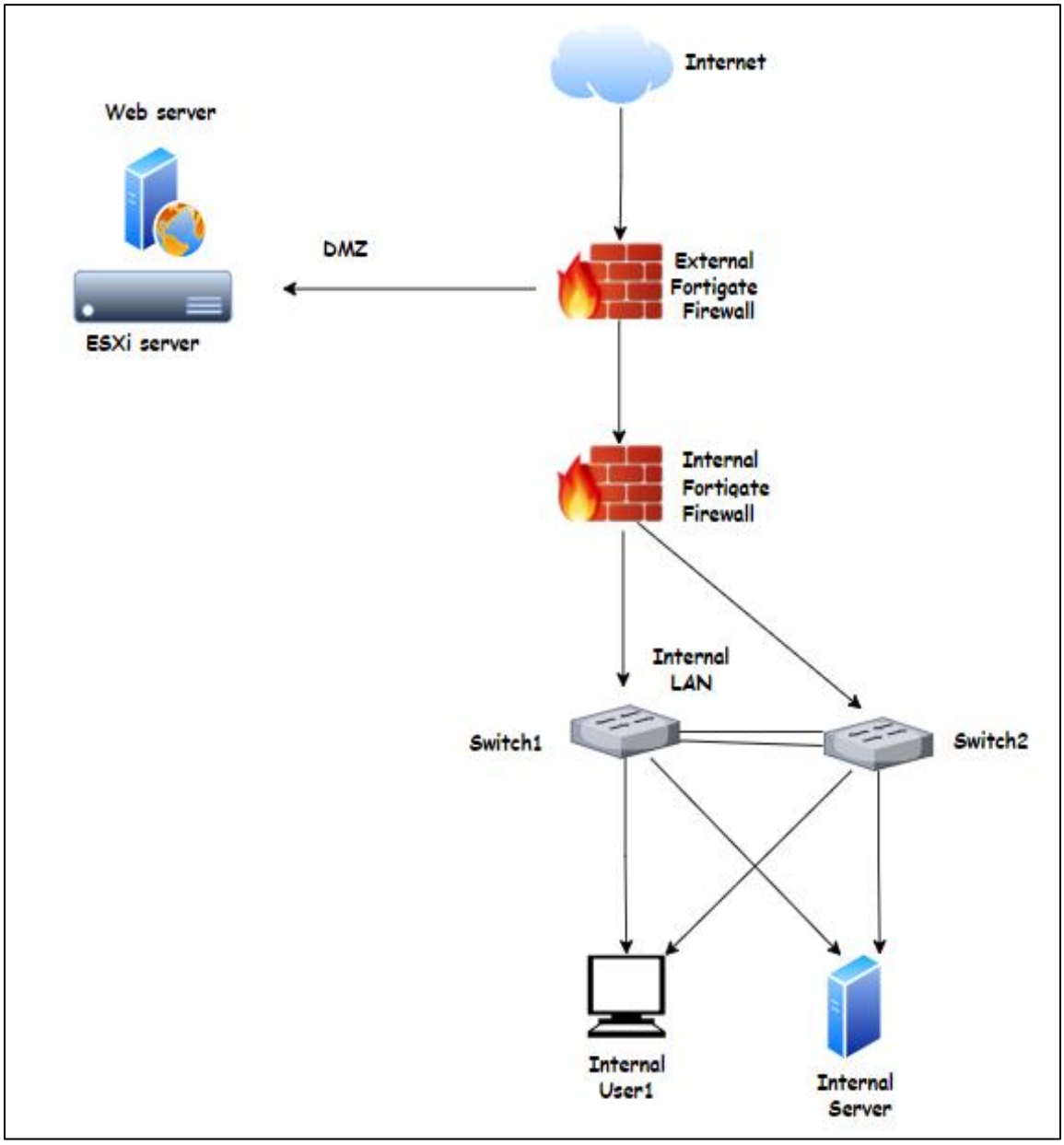


Figure 196 Draft proposal design presented to the client.

8.5.4. Initial developed system design

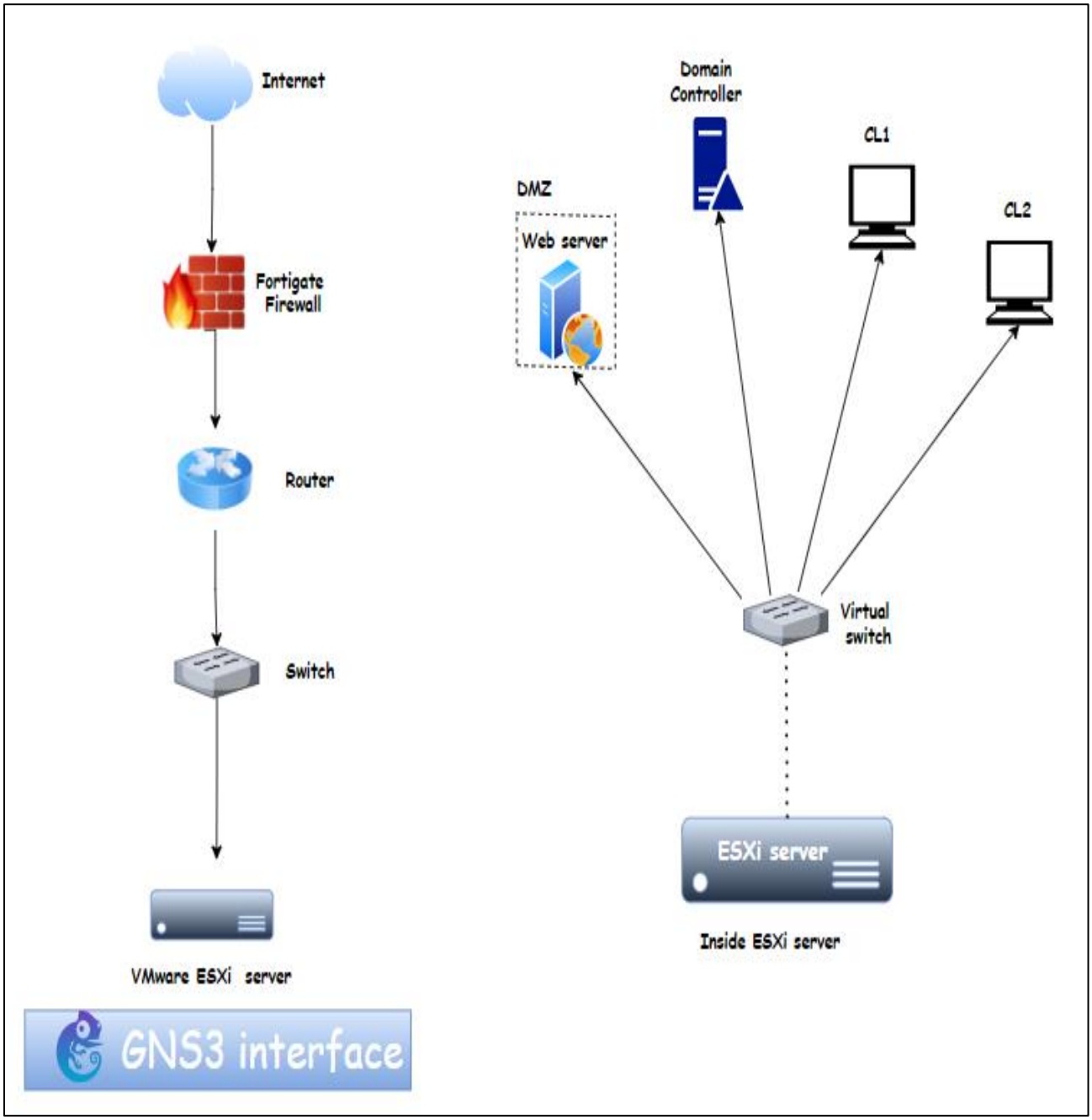


Figure 197 Design used for the initial development of the system.

8.6. Appendix E: User Feedback

8.6.1. User initial requirement gathering.

A short Q/A text conversation for collecting user's requirement.

Client Name: Everest Bank Pvt. Ltd.

Project Topic: Network design and implementation, enhancing internal network security.

1. What methods do you use for the security of your network?

➔We have been using a firewall for the network security of the organization.

2.Have you ever experienced any hardware failure in the past that have impacted your network availability or cause data loss?

➔Potentially, we have not faced any hardware failure in the past. We have multiple network devices configured for hardware failover.

3. How are you currently managing you network assets?

➔We perform manual management of the network assets in some monthly gap. The management of the assets has been a headache and time-wasting task.

4. How it would be to isolate the external service provided components and restrict the access to your internal network using DMZ?

➔It would be nice approach.

5. Would you be willing to utilize the DMZ implementation on your network?

➔ Yes, if it will be able to enhance our system's security, we will surely want to approach this.

4. Are you open to implement automated asset scanning and management software deployment?

➔Yes, it would be a great idea.

8.6.1. Pre-meeting for the feedback of initially developed system.

Client pre-meeting about the project

Client Name: Everest Bank Pvt. Ltd.

Agenda: Meeting to feedback about initially developed system and additional requirement

Q/ A session

1. How useful and convenient did you find Lansweeper for asset scanning, monitoring and management?

➔We found it very convenient and useful to do asset scanning and management.

2. How useful you found the implementation of domain controller for managing users and policies?

➔We were already using ADDS, but the implementation of the Lansweeper under domain controller proved to be extremely useful for us.

3. Do you like the remote access policies that have been configure on Domain controller?

➔Yes, it has limited remote access from many users to the main server.

4. Was it possible for IT officers to remotely access the Domain Controller?

➔Yes, our specific IT officers were successfully able to remote access the domain controller.

5. Do you have any additional requirement to implement in this system?

➔Not sure, but we have a hectic problem of software installation. This task has consumed our lots of time.

6. How it would be to implement an automated software installation and patch management tool?

➔ It would be a very great idea.

.

8.6.2. Post meeting about the final developed system.

Client pre-meeting about the project

Client Name: Everest Bank Pvt. Ltd.

Agenda: Meeting for reviewing the final developed system.

1. Have you noticed any improvements in system's security since the implementation of DMZ?

➔Yes, the system is felt to be more secure now.

2. How useful and convenient was it to use PDQ deploy for automatic software installation and patch management?

➔ It was quite easy to deploy the packages and update packages. This tool is the best choice for eliminating the time-consuming software installations.

3. Do you find the system use-friendly?

➔ Yes, this system is user friendly and also seems to be an easy implementation.

4. Do you experienced any functionality error/

➔ Not yet.

5. Are there any additional requirement that can be made to improve your network?

➔ No, the system is quite good.

6. Are you satisfied with the developed system?

➔ Yes, I am fully satisfied with the developed system.

8.7. Appendix F: Software requirements description

- Gantt Project

  The Gantt project tool is a software that aids in project management by creating Gantt charts that illustrates project schedules, tasks relationships and resource allocations. These charts display tasks, start and end dates and the independencies between tasks. The tool allows users to divide a project into tasks and sub-tasks, assign resources, set task durations and dependencies, and track progress against the project plan (Grant, et al., 2022).

- GNS3 and GNS3 VM

  GNS3 is an open-source simulation and design software that allows users to create and test complex network topologies virtually. It uses real network operating systems to emulate the behavior of network devices and allows users to drag and drop devices onto a virtual canvas to build a virtual network (Bagci, 2022).

  GNS3 VM is a software program that facilitates network simulation and design. It is essentially a preconfigured virtual machine image that can be installed on various virtualization platforms such as virtual box, VMware or KVM. It is used in combination with the GNS3 software application to create complex network topologies and simulate different network environments (gns3, 2023).

- VMware Workstation 16

  VMware workstation 16 is a desktop virtualization tool that enables users to create and run multiple virtual machines on a single physical machine. It allows for easy management of virtual machines, including cloning, snapshots and restoring VMs, and supports a variety of operating systems, including Windows, Linux, and macOS. Users can simulate different software configurations and network environment and run multiple virtual machines simultaneously, sharing resources between them. The software is commonly used by developers for testing and debugging software applications (Braden, 2021).

- VMware ESXi 7

  VMware ESXi is a server-side bare-metal hypervisor that can create one or more virtual machines using physical hardware (VMs). It is a hypervisor that interfaces with agents that run on top of it and is independent of the operating system (Feilz, 2022).

- Firewall

  A firewall is network security device that monitors the incoming and outgoing network traffic and permits or denies data packets based on a set of security rules. Its main purpose is to create a barrier between internal network and incoming traffic from external sources (Deshpande, 2022).

- Router

  Routers are the network devices that connects two different networks. Its main aim is to manage traffic between these networks by forwarding data packets to the destination IP address and allowing multiple devices to use the same internet connection (Fisher, 2021).

- Switch

  A switch is a device used in a local area network to enable communication between multiple devices by forwarding data packets. There are two types of switches-managed and unmanaged. Managed switches allow for network control and configuration of VLANs, QoS and security, while unmanaged switches are simple plug-and-play devices that don't require any configuration (Singh, 2022).

- Windows server 2019 and 2022

  A computer program/ device that provides a service to another computer program is called server. Server stores, sends, and receives the data. A computer, any software tool can act as server if it provides different services. Windows server is an operating system developed by Microsoft business purposes, which lacks consumer applications but provide tools for administrators. It is suitable for companies that prioritize security and require customer support or rely other Microsoft services (Bender, 2023).

- Debian 11 Linux

  Debian 11 is an open-source Linux distribution and the newest version of the Debian Operating system. It was launched in August 2021 and includes new features such as improved security, updated software packages and a better installation experience. The default desktop environment is GNOME 3.3.8 and it uses the Wayland display server. Debian 11 is a stable, reliable and can be used on servers, desktops, and embedded devices (BANGER, 2023).

- Microsoft office

  Microsoft office is s set of software tools created by Microsoft that are used for productivity. It includes different programs such as Word, Excel, PowerPoint, Outlook, Access, Publisher, and OneNote, among others. In this project Microsoft tools such as MS word and PowerPoint has been used. Microsoft word is a word processing software application, widely used for creating, editing, and formatting text documents. Microsoft PowerPoint is a presentation software that is part of the Microsoft office suite, used for creating slide-based presentations for designing visually appealing presentations (Rouse, 2020).

8.8. Appendix G: Client approval letter

एभरेष्ट बैंक लिमिटेड
EVEREST BANK LIMITED
(A Joint-Venture with punjab national bank, India)
Consistent, Strong & Dependable
(नेपाल राष्ट्र बैंकबाट 'क' वर्गको इजाजतपत्र प्राप्त संस्था)

14th December ,2022

Letter of approval for designing and implementing network diagram for network security

Dear Janaki Chaudhary,

I am writing to recommend your network design to be implemented in our organization.

As per your proposal, we seem to like your project for our organization's IT system , that will provide security to our organization as well as alter our IT department to be safe from untrusted external network. Our organization has shown interest in implementing your system to provide security against cyber threats and enhance our organization's network features.

Sincerely,

Prabin Subedi

Branch Manager

Lamahi Branch, Lamahi MCP-05, Dang

9811535981, 082-540802

Prabin.subedi@ebl.com.np

EVEREST BANK LTD. Lamahi Branch Dang, Nepal

Figure 198 Client's approval letter.