



# Noroff

School of technology  
and digital media

Name	Maximilian Galcso
Project Name	Project 07 - Startup Company
Course	NSA-Online 08.2023. PT

## Table of Contents

Table of Contents .....	2
1. Introduction .....	4
2. Project Plan .....	5
A. SMART Goals .....	5
B. Critical Path Summary .....	5
C. Milestones .....	6
2.1. User Roles and Access Control .....	7
2.2. Azure Integration Strategy .....	9
2.3. Backup and Resilience .....	10
2.4. Security Measures .....	10
A. Network segmentation via VLANs .....	11
B. PfSense firewall rules .....	11
C. Group Policy Objects (GPOs) .....	12
D. Role-based access control .....	12
E. Organizational Units (OUs) .....	13
F. Password policy and first-login behavior .....	14
G. Active Directory: Users and Organizational Structure .....	15
2.5. Site C (Client-Face Office) and Guest Segregation .....	17
3. Technical Deployment and System Setup .....	18
3.1. Network topology and VLAN allocation .....	18
3.2. Active Directory and Windows Server Configuration .....	20
3.3. Windows 10 Client – Domain Join and Connectivity Test .....	21
3.4. Linux Fedora Workstation & Server Domain Join .....	23
3.5. Azure File Sharing and VPN Configuration .....	26
3.6. Correction, Reproduction .....	29
A. HDD Assignment to Domain Controller .....	29
B. Folder Structure and Permissions .....	29
C. Marketing Materials Copying .....	30
D. SMB Sharing of Site ABC Drive .....	31
E. Guest Access Demonstration .....	32
F. PfSense VLAN70 Configuration .....	32
G. Guest VM Setup and Access .....	33
3.7. Mounting SMB File Share on Linux Machines .....	34
A. Integrating Permissions on Fedora Machine .....	34

B. Preparing for Mount and One-Time Mount Operation .....	35
C. Persistent Mount via /etc/fstab .....	36
D. Verification and Usage .....	37
3.8. PfSense Firewall Installation and Configuration .....	38
4. Limitations, Conclusions, and Recommendations .....	41
4.1. What I Learned During the Project .....	41
4.2. New Tools and Technical Challenges .....	41
4.3. What Went Smoothly and What Caused Difficulty .....	42
4.4. Reflection and Self-Evaluation .....	43
4.5. Future Improvements and Recommendations .....	44
Bibliography .....	46

## 1. Introduction

This project aims to design and implement a hybrid IT infrastructure for a startup company across three distinct sites (Site A, B, and C), enabling secure and well-segmented file sharing between them. The solution incorporates Azure cloud storage and security services to ensure flexible access and data protection.

As part of the project, a test environment is created using VMware Workstation, consisting of a PfSense firewall, Windows Server 2022, Windows 10, Fedora Server (with KDE Plasma GUI), and Fedora Workstation. This environment includes the configuration of Active Directory, DNS, and various GPO policies with department-specific restrictions. In addition, an Azure environment is set up, featuring a Windows Server VM and Azure File Shares. One share is used for inter-site collaboration, while a separate read-only file share is dedicated to guest access.

The document is structured as follows: I present the business environment and key components after the introduction, followed by a detailed explanation of the technical implementation. The closing section includes an evaluation of the results, reflections on encountered challenges, and lessons learned.

Anticipated technical challenges include the correct sequence of network setup steps, the precise application of GPOs to different departments, domain joining of Fedora machines, firewall rule configuration, and domain integration and accessibility of the Azure VM. The project has been planned to ensure the system is feasible, scalable, and secure in a real-world scenario.

This initiative addresses the startup's need for a robust, scalable IT infrastructure to support seamless operations across three geographically dispersed sites. By leveraging Azure's cloud capabilities and on-premises virtualization, the project ensures efficient file sharing, robust security, and streamlined management. The test environment simulates real-world conditions, allowing validation of network configurations, security policies, and cross-platform integration. Key objectives include achieving secure inter-site collaboration, enforcing department-specific access controls, and ensuring guest access to designated resources. The project also emphasizes scalability to accommodate future growth and adaptability to evolving security threats, providing a practical blueprint for modern hybrid IT deployments.

## 2. Project Plan

### A. SMART Goals

- **Specific:** The project aims to simulate a corporate network across three sites using Cisco Packet Tracer and to test a real VMware-based Active Directory environment with both Windows and Fedora machines.
- **Measurable:** Each core functionality — such as DNS, AD replication, file sharing, PfSense firewall rules, and Azure Storage integration — will be successfully tested at least once.
- **Achievable:** All components of the project are either already functional or easily installable. The lab and software environments (VMware, Cisco PT, Azure) are available.
- **Relevant:** The project focuses on building a secure, scalable hybrid infrastructure suitable for business use. While educational, it follows real-world industry practices.
- **Time-bound:** All tasks will be completed by June 8, 2025, following a predefined daily and weekly schedule.

### B. Critical Path Summary

CPT → VLAN & IP configuration → PfSense firewall rules → Domain setup → Azure file access → BYOD GPO implementation → Testing → Documentation

### C. Milestones

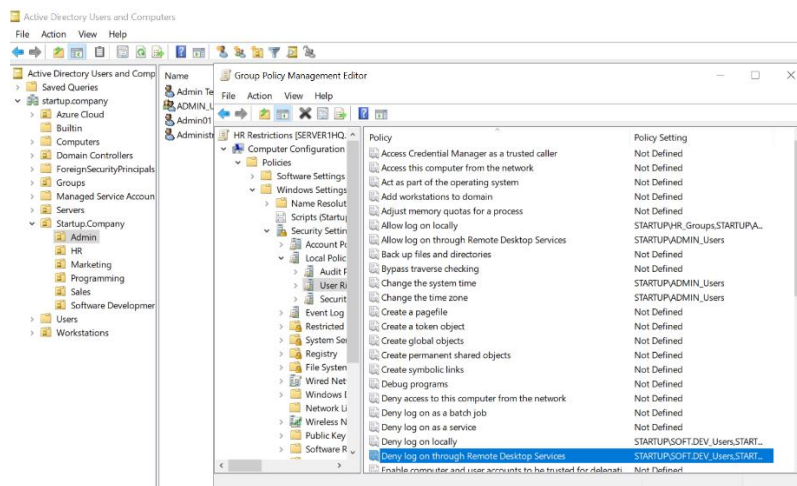
No. Milestone	Description	Deadline
1. Project Initiation	Requirements, objectives, documentation, preparation	2024.04.07
2. Basic Topology (CPT)	VLANs, subnets, and routing draft in Cisco Packet Tracer	2024.04.20
3. VMware Environment	VM installation (Windows + Fedora), AD Domain setup, client connection	2024.04.28
4. Network Refinement	ACLs, PfSense firewall, DNS/DHCP servers, BYOD, VPNs	2024.05.15
5. Integration Testing	A logical simulation between CPT and VMware, Azure/cloud connectivity	2024.05.25
6. Go-Live Simulation	"Live" trial run, troubleshooting, documentation template upload	2024.06.01
7. Project Closure	Final presentation, submission of documentation	2024.06.06

## 2.1. User Roles and Access Control

Each department was assigned its own VLAN, organizational unit, and group, with users allocated accordingly. Department-specific Group Policies (GPOs) were implemented, including user permissions and device usage restrictions.

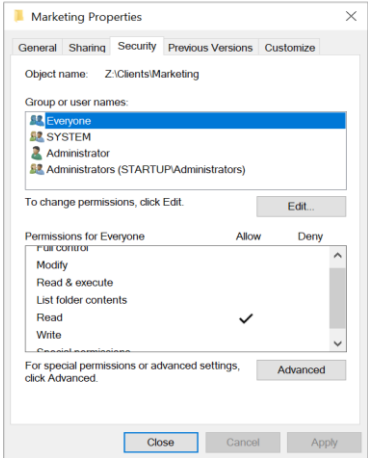
- Admins have full access to both local and cloud systems and can log into and manage any machine.
- HR, Marketing, Developers (Programming / Software Development), and Sales can only access the shares related to their department.

Sales, except for BYOD users, have restricted access even within their system as shown in the picture below.



- Guests at Site C have read-only permission to an Azure share containing a copy of marketing materials, accessed via a guest network.

Name	Date modified	Type	Size
Marketing	5/31/2025 17:37	File folder	



The guest network (VLAN 70) cannot reach the domain due to restrictions and firewall rules, further enhancing network security.



## 2.2. Azure Integration Strategy

Azure was selected as the cloud platform due to its seamless integration with Windows Server environments and its availability for educational use. Additionally, during the NSA course, we studied it in the Cloud Computing Foundation module, where I became familiar with its user-friendly interface and built-in security features, which I found especially compelling.

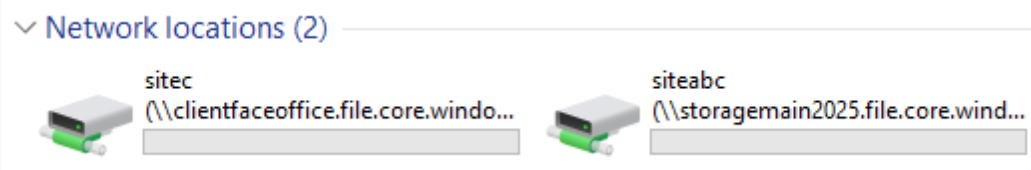
The decision to implement a hybrid infrastructure was since, for a startup, cost-effective scalability, high availability, and secure data handling are essential. Instead of relying entirely on an on-premises or fully cloud-based solution, the hybrid model allows critical systems—such as Active Directory—to remain on-premises. At the same time, file sharing and backups are moved to the cloud. This provides flexibility to adapt to future business growth. This approach was particularly important for Site C, where a guest network had to be isolated and provided with read-only access to shared resources.

To estimate the monthly cost of the Azure-based components, I used the Azure Pricing Calculator, as shown in the screenshot below.

Microsoft Azure Estimate						
Your Estimate						
Service category	Service type	Custom name	Region	Description	Estimated monthly cost	Estimated upfront cost
Compute	Virtual Machines		Norway East	1 A1 v2 (1 Core, 2 GB RAM) x 730 Hours (Pay as you go), Windows (AHB), OS Only, 0 managed disks – S4; Inter Region transfer type, 5 GB outbound data transfer from Norway East to Norway West	kr334,85	kr0,00
Storage	Storage Accounts		Norway East		kr0,00	kr0,00
Storage	Azure Files		Norway East	HDD (Standard) Media tier, LRS Redundancy, Provisioned v2 Billing model, Provisioned capacity – 256 GiB, Provisioned storage, 1,052 Provisioned IOPS, 66 MB/sec Provisioned throughput, Used capacity – 0 GiB Overflow used snapshot storage, 0 GiB Used soft-deleted storage, 0 File sync servers	kr700,99	kr0,00
Storage	Azure Files		Norway East	HDD (Standard) Media tier, LRS Redundancy, Provisioned v2 Billing model, Provisioned capacity – 256 GiB, Provisioned storage, 1,052 Provisioned IOPS, 66 MB/sec Provisioned throughput, Used capacity – 0 GiB Overflow used snapshot storage, 0 GiB Used soft-deleted storage, 0 File sync servers	kr700,99	kr0,00
Storage	Storage Accounts		Norway East		kr0,00	kr0,00
Support			Support		kr0,00	kr0,00
			Licensing Program	Microsoft Customer Agreement (MCA)		
			Billing Account			
			Billing Profile			
			Total		kr1 736,83	kr0,00
Disclaimer						
All prices shown are in Norway – Krone (kr) NOK. This is a summary estimate, not a quote. For up to date pricing information please visit <a href="https://azure.microsoft.com/pricing/calculator/">https://azure.microsoft.com/pricing/calculator/</a> . This estimate was created at 6/7/2025 2:49:31 PM UTC.						

The hybrid approach includes the following Azure components:

- Two Azure File Shares, which enable centralized file access across multiple sites
- Azure Backup, used for long-term storage and disaster recovery purposes
- An Azure Virtual Machine, running a Windows Server instance joined to the on-premises domain



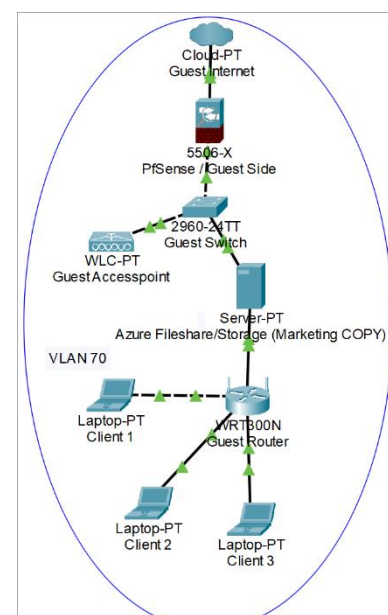
## 2.3. Backup and Resilience

In this project, the local shares are backed up within the Azure cloud, where the Storage Accounts include built-in backup solutions that automatically handle data protection and recovery. This approach significantly enhances the overall security of the system.

In case of local data loss or hardware failure, the backups allow for quick restoration of the data.

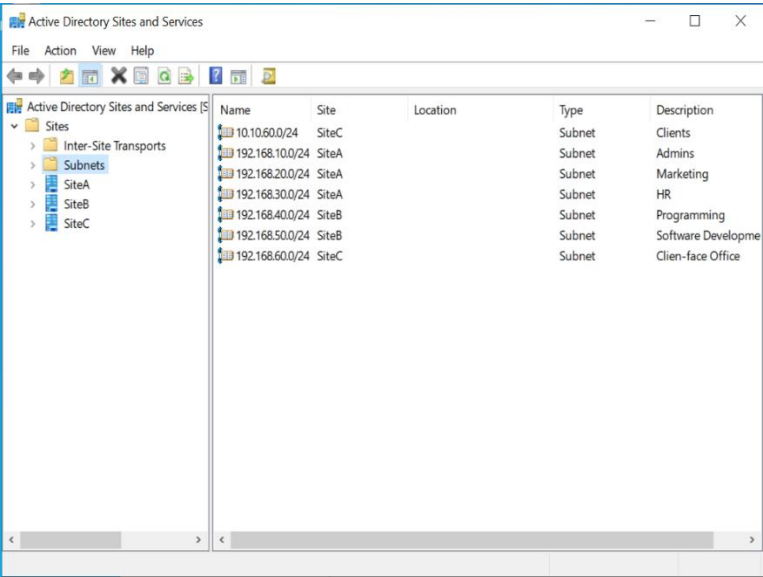
## 2.4. Security Measures

I chose the PfSense firewall to ensure network security because it is free, and easy to manage, and I recall reading somewhere — possibly on a forum or in documentation — that it is a good solution for beginners and smaller projects. This was especially important for blocking the guest network on Site C (10.10.60.024), as mentioned in the Introduction, to protect internal resources. During my research, I did not evaluate many other firewalls because PfSense's web interface is straightforward to configure, allowing me to quickly set up rules to restrict traffic. Being free, it can run on existing hardware or be installed on an inexpensive virtual machine (VM), which offers cost efficiency ideal for a startup environment.



Key security solutions implemented to protect the infrastructure include:

**A. Network segmentation via VLANs:** Each department is assigned a dedicated VLAN (e.g., VLAN10 for Admin, VLAN20 for Marketing), providing network-level isolation and reducing exposure to lateral threats.

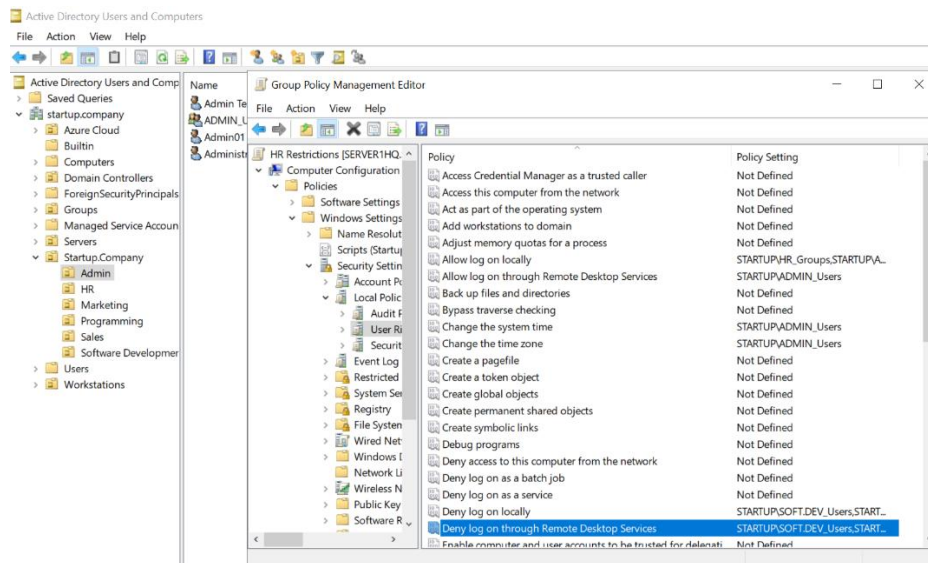


**B. PfSense firewall rules:** The firewall strictly separates the guest network (VLAN70) from all domain-connected VLANs. Traffic from the guest network is blocked from reaching internal domain resources, ensuring a secure perimeter.

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input type="checkbox"/>	32/139 KiB	IPv4 *	VLAN70 subnets	*	*	*	*	none		Allow full internet for guest		
<input type="checkbox"/>	0/371 KiB	IPv4 *	VLAN70 subnets	*	*	*	*	none		Catch-all		
<input type="checkbox"/>	0/0 B	IPv4 *	VLAN70 subnets	*	VLAN70 subnets	*	*	none		Peer-to-Peer block		
<input type="checkbox"/>	0/0 B	IPv4 *	VLAN70 subnets	*	LAN address	*	*	none		VLAN 10,20,30,40,50,60 block		
<input type="checkbox"/>	0/0 B	IPv4 *	VLAN70 address	*	192.168.10.0/24	*	*	none				
<input type="checkbox"/>	0/0 B	IPv4 TCP	VLAN70 subnets	*	*	80 - 443	*	none		Allow web		
<input type="checkbox"/>	0/0 B	IPv4 UDP	VLAN70 subnets	*	*	53 (DNS)	*	none		Allow DNS		
<input type="checkbox"/>	0/0 B	IPv4 TCP	VLAN70 subnets	*	WAN subnets	445 (MS DS)	*	none		Azure File Share SMB access		

## C. Group Policy Objects (GPOs):

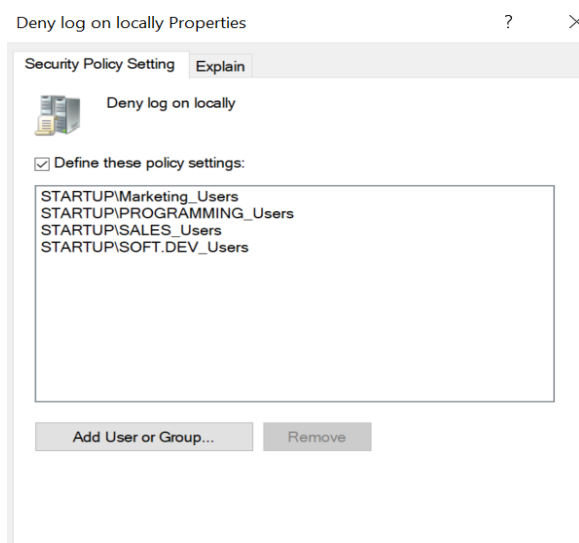
User environments are restricted using GPOs. These define what resources users can access, limit access to system settings.



## D. Role-based access control:

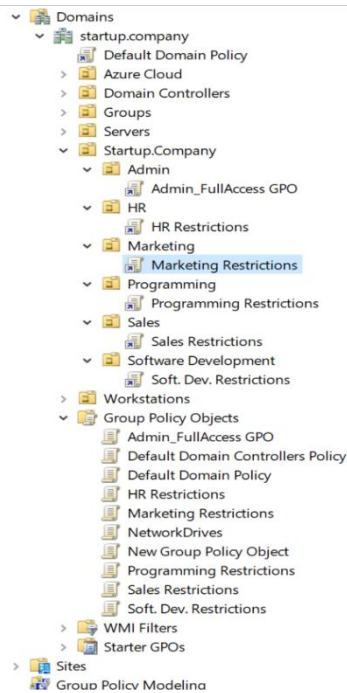
- Only users assigned to a specific department have access to that department's workstations and resources.
- Users from one department cannot log into machines belonging to another department.

The image below shows the login restriction applied to the HR department.



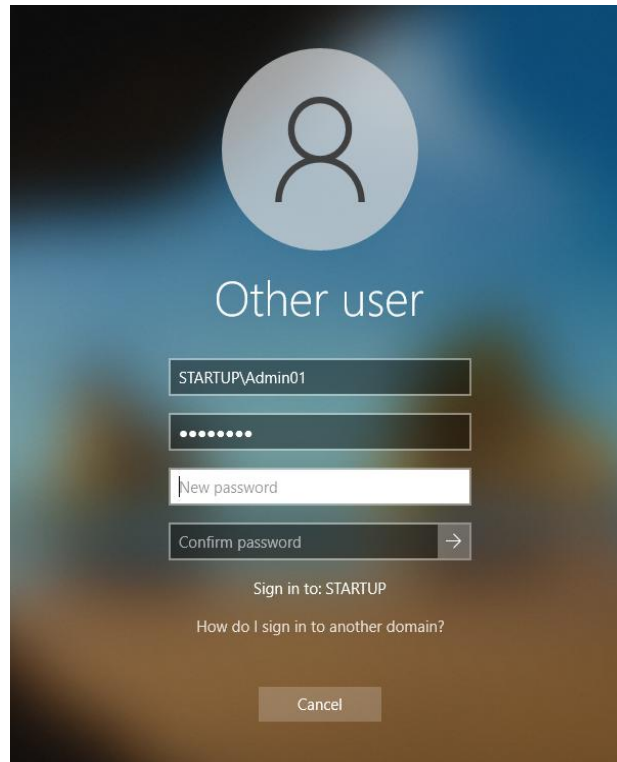
- c. Only designated Admin users are allowed remote access (RDP), while standard users are restricted from remote logins.
- d. Only specific roles (typically Admins) can shut down or restart machines.
- e. Time and timezone modification is restricted to administrative users only.

**E. Organizational Units (OUs):** GPOs are linked to OUs that represent each department.

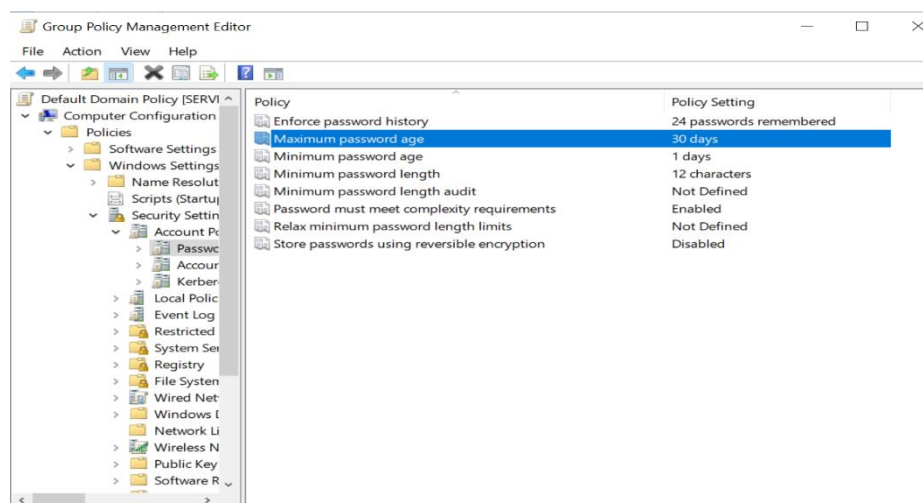


## F. Password policy and first-login behavior:

- a. All new users are required to change their password at first login.



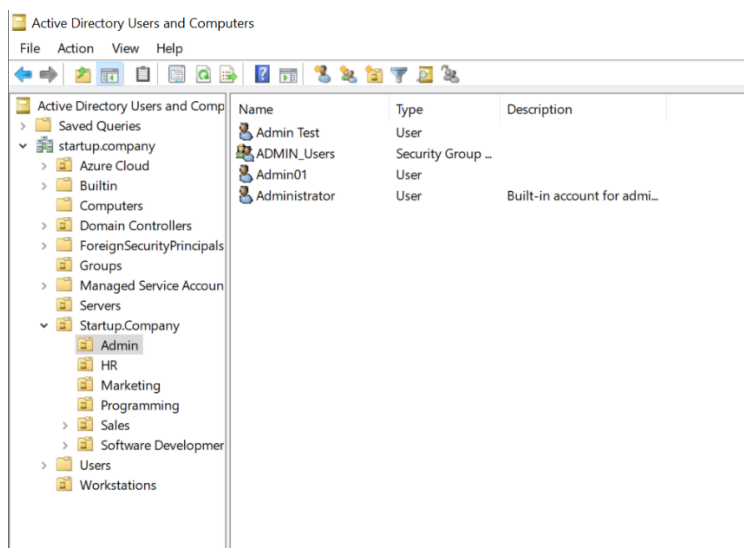
- b. Passwords must meet complexity requirements: a minimum of 12 characters, including at least one uppercase letter, one lowercase letter, one number, and one special character.
- c. Passwords are set to expire every 30 days, requiring users to update them regularly to enhance security.



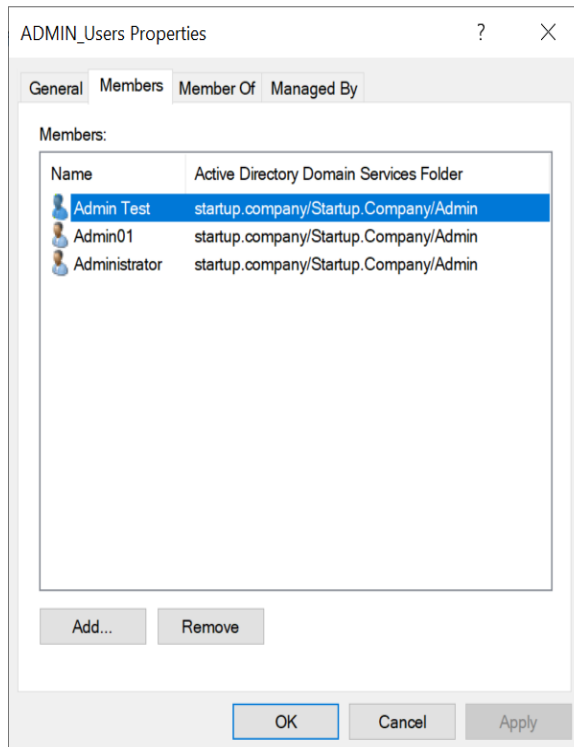
## G. Active Directory: Users and Organizational Structure

Within the Active Directory Users and Computers (ADUC) console, under the domain startup.company, several top-level Organizational Units (OUs) were created to provide clear structural and administrative separation. These include Servers, Workstations, Azure\_Cloud, and a central OU named startup.company, which holds all user- and department-related OUs.

Inside the startup.company OU, individual sub-OUs were created for each department: Admin, HR, Marketing, Programming, Sales, and Software Development. Each department OU contains at least one test user account (Admin01, HR01, Marketing01, etc.), which were used to validate Group Policy Objects (GPOs), group-based access, and login functionality.



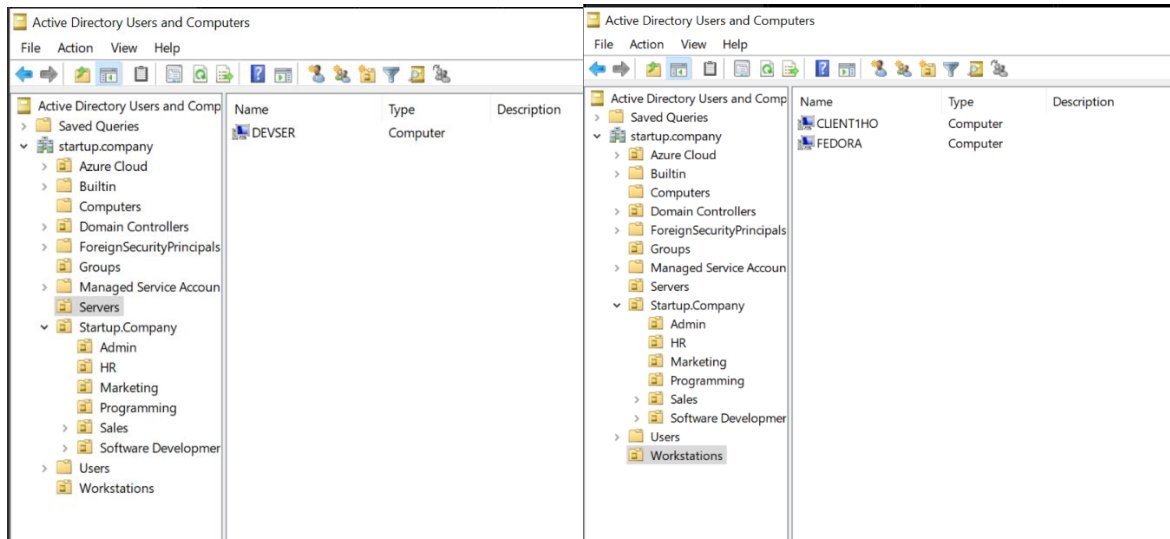
For proper access management, separate global security groups were created for each department (Admin\_Users, HR\_Users, Marketing\_Users, Sof.Dev.\_Users, Programming\_Users, Sales\_Users). All user accounts were added to their corresponding group. This allows GPOs, file share permissions, and network access controls to be applied efficiently and consistently at the group level rather than individually per user.



Client machines were placed under the Workstations OU, while server machines were placed under Servers. Additionally, any machines that were domain-joined from Azure were moved into the Azure\_Cloud OU to maintain structural clarity and prepare for potential hybrid management policies.

This organized OU and group structure provides a scalable, manageable, and secure foundation for enterprise-level Active Directory operations.





## 2.5. Site C (Client-Face Office) and Guest Segregation

Site C operates as an isolated zone.

Guests connecting here are not joined to the domain and access the network via Wi-Fi or other isolated connections.

Firewall rules ensure that they can only access a specific copy of an Azure file share with read-only permissions.

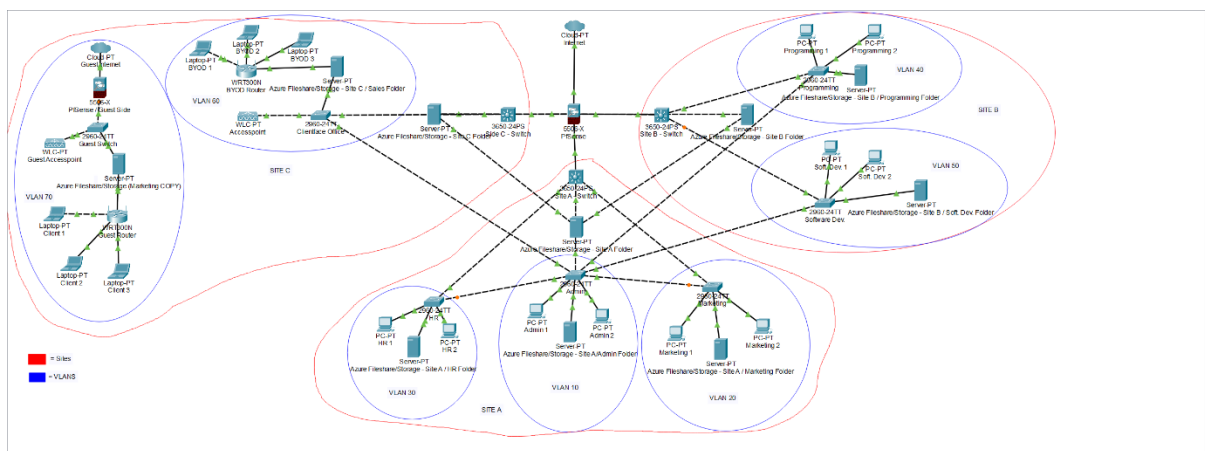
Due to technical issues, a VPN connection could not be established (this will be explained in more detail in a later chapter).

### 3. Technical Deployment and System Setup

#### 3.1. Network topology and VLAN allocation

After defining the project objectives in the introduction, I used Cisco Packet Tracer to build a hybrid infrastructure simulating three separate company sites: Site A, B, and C.

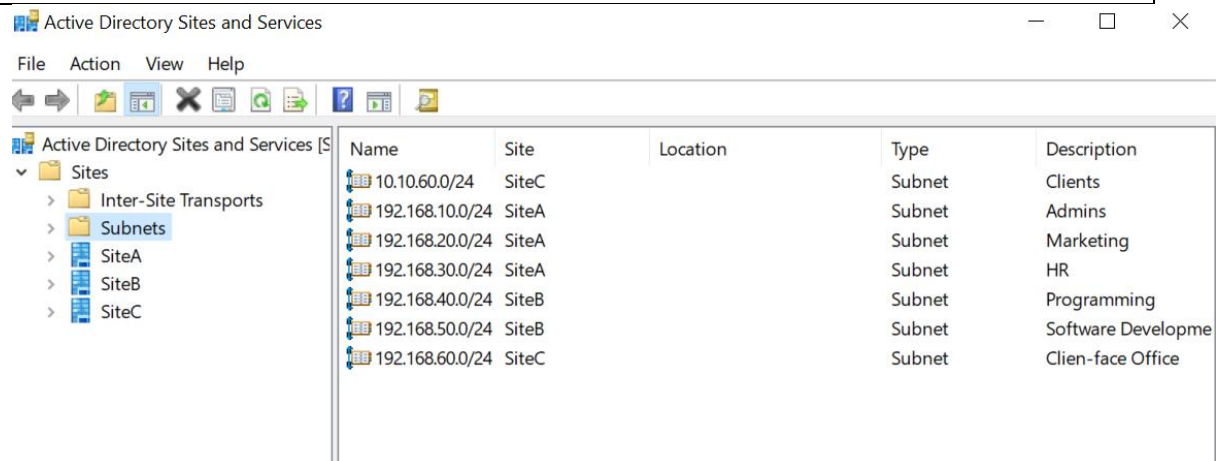
I configured multiple VLANs (10, 20, 30, 40, 50, 60, 70), each corresponding to a specific department: Admin, HR, Marketing, Programming, Software Development, BYOD/Client-Face Office, and Guest.



Cisco Packet Tracer topology showing the VLAN configuration.

This image demonstrates that the network logically separates Site C for security purposes. Below the topology, the planned IP address allocation for each VLAN is also presented.

VLAN	Depart	Location	IP Addresses	DHCP Scopes
10	Admin	Site A	192.168.10.0/24	192.168.10.100–200
20	Marketing	Site A	192.168.20.0/24	192.168.20.100–200
30	HR	Site A	192.168.30.0/24	192.168.30.100–200
40	Programming	Site B	192.168.40.0/24	192.168.40.100–200
50	Software Development	Site B	192.168.50.0/24	192.168.50.100–200
60	Client-Face Office /Sales	Site C	192.168.60.0/24	192.168.60.100–200
70	Guest	Site C	10.10.60.0/24	10.10.60.100–200



## 3.2. Active Directory and Windows Server Configuration

After installing Windows Server, I performed a full system update using Windows Update and renamed the machine to Server1HQ.

### About

Your PC is monitored and protected.

[See details in Windows Security](#)

### Device specifications

Device name	Server1HQ
Processor	AMD Ryzen 9 5900HX with Radeon Graphics 3.29 GHz (2 processors)
Installed RAM	2.00 GB
Device ID	1D235F3D-FA43-46DA-836A-7A4DCC7F13D0
Product ID	00454-40000-00001-AA256
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Copy

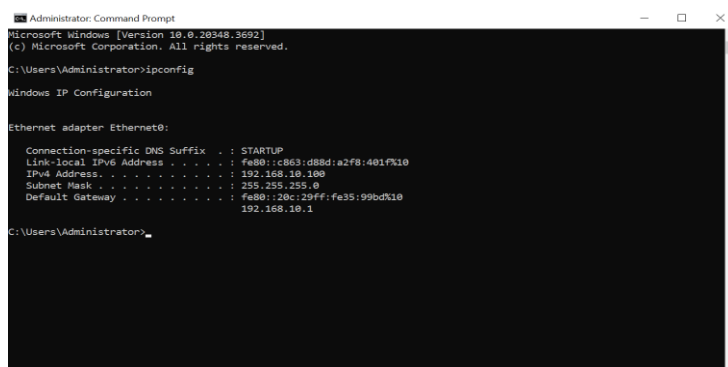
Rename this PC

Following this, I used Server Manager to install the Active Directory Domain Services (AD DS) and DNS Server roles.

Next, I opened Command Prompt and ran the ipconfig command to verify the current IP configuration. I also ran ncpa.cpl to access the Network Connections window. There, I right-clicked the active network adapter, selected Properties, then selected Internet Protocol Version 4 (TCP/IPv4) and clicked on Properties.

Based on the ipconfig output, I manually entered the following values:

- **IP Address: 192.168.10.100**
- **Subnet Mask: 255.255.255.0**
- **Default Gateway: 192.168.10.1**



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.3892]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

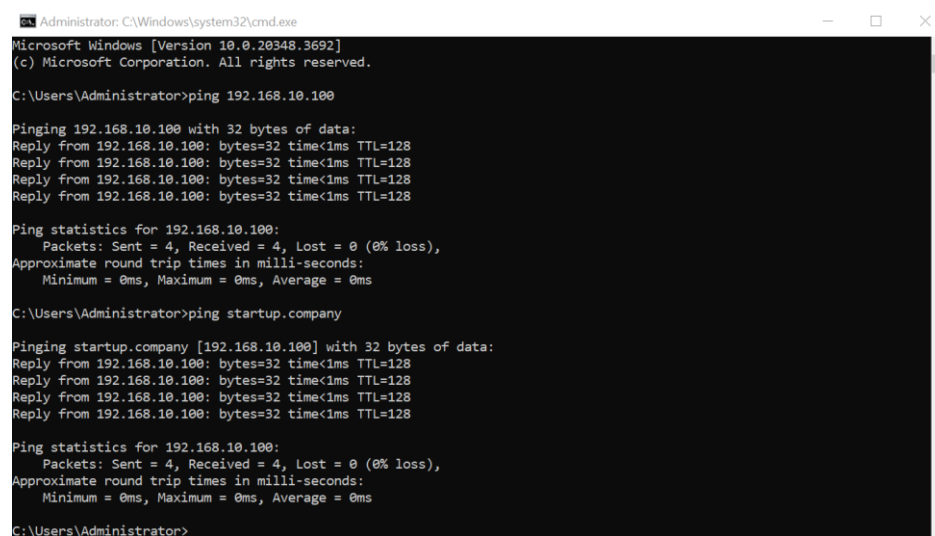
    Connection-specific DNS Suffix  . : STARTUP
    Link-local IPv6 Address . . . . . : fe80::c863:d88d:a2f8:401f%10
    IPv4 Address. . . . . : 192.168.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::28c:29ff:fe35:99bd%10
                                192.168.10.1

C:\Users\Administrator>
```

In the Preferred DNS Server field, I entered the IP address of the server itself.

As the next step, I promoted the server to a Domain Controller. During this process, I created a new forest and domain with the name startup.company. Once the promotion was completed, the server automatically rebooted.

After the reboot, I opened Command Prompt again and used the ping command twice to test connectivity: first to the Domain Controller's IP address, and second to the domain name itself (startup.company) to verify DNS resolution.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.3692]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping startup.company

Pinging startup.company [192.168.10.100] with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

### 3.3. Windows 10 Client – Domain Join and Connectivity Test

After the domain controller was set up, I installed a Windows 10 virtual machine and renamed it to Client1HO.

#### About

Your PC is monitored and protected.

[See details in Windows Security](#)

#### Device specifications

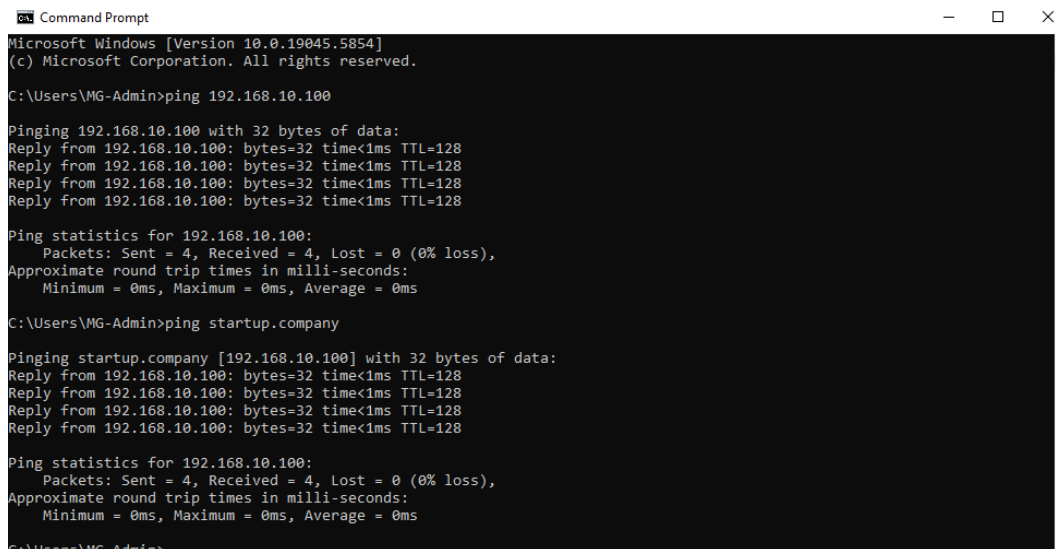
Device name	Client1HO
Full device name	Client1HO.startup.company
Processor	AMD Ryzen 9 5900HX with Radeon Graphics 3.29 GHz (2 processors)
Installed RAM	2.00 GB
Device ID	ACA4F12B-5439-41C1-9123-0FA78FD24742
Product ID	00329-20000-00001-AA099
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Copy

Rename this PC

I opened Command Prompt and ran the following commands:

- ping Server1HQ – to confirm hostname resolution via DNS
- ping startup.company – to verify domain-level connectivity



```
Microsoft Windows [Version 10.0.19045.5854]
(c) Microsoft Corporation. All rights reserved.

C:\Users\MG-Admin>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\MG-Admin>ping startup.company

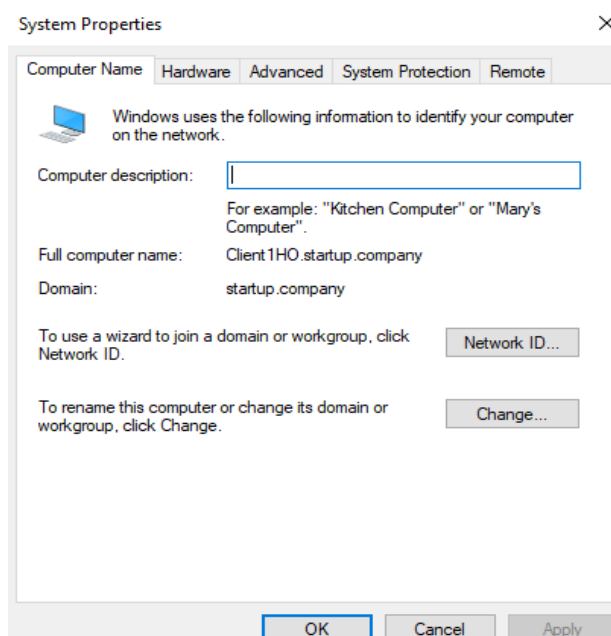
Pinging startup.company [192.168.10.100] with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128
Reply from 192.168.10.100: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\MG-Admin>
```

I then opened the Rename this PC (advanced) menu and chose the Rename this Computer or Change its Domain or Workgroup menu and clicked on the bottom next to it.

I joined the machine to the domain startup.company using domain credentials.



After successfully joining the domain, the machine was restarted.

### 3.4. Linux Fedora Workstation & Server Domain Join

As the first step, I changed the hostname of the Linux machine using the command:

***sudo nano /etc/hostname***

The hostname was set to fedora.startup.company.

Next, I joined the machine to the domain using the following command:

***sudo realm join startup.company -v***

(If the hostname is not set manually beforehand, the system will automatically generate one during the join process.)

After executing the command, the system prompts for a domain user account with the necessary permissions. If no error message appears, it means the machine has successfully joined the domain.

The two attached screenshots show the Fedora Server (left) and Workstation (right) after the domain join. Both successfully pinged the domain controller, and the realm list command confirmed the domain membership. The ip a command was also used to verify the current IP configuration.

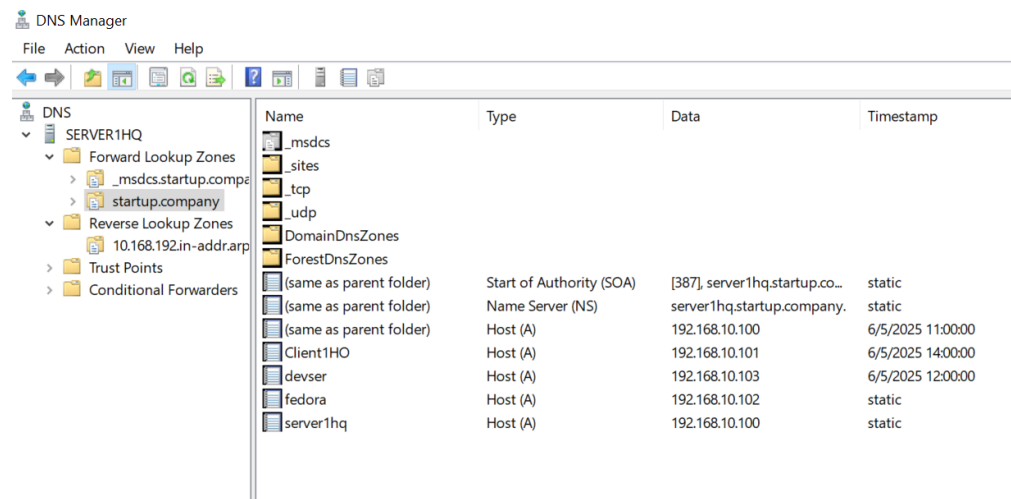
```

devos@devserver:~$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=128 time=0.448 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=128 time=0.439 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=128 time=0.754 ms
64 bytes from 192.168.10.100: icmp_seq=4 ttl=128 time=0.376 ms
64 bytes from 192.168.10.100: icmp_seq=5 ttl=128 time=0.336 ms
64 bytes from 192.168.10.100: icmp_seq=6 ttl=128 time=0.447 ms
64 bytes from 192.168.10.100: icmp_seq=7 ttl=128 time=0.411 ms
64 bytes from 192.168.10.100: icmp_seq=8 ttl=128 time=0.347 ms
64 bytes from 192.168.10.100: icmp_seq=9 ttl=128 time=0.418 ms
64 bytes from 192.168.10.100: icmp_seq=10 ttl=128 time=0.382 ms
64 bytes from 192.168.10.100: icmp_seq=11 ttl=128 time=0.517 ms
^C
--- 192.168.10.100 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10261ms
rtt min/avg/max/mdev = 0.336/0.443/0.754/0.109 ms
devos@devserver:~$ realm list
startup.company
type: kerberos
realm-name: STARTUP.COMPANY
domain-name: startup.company
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: sssd-common
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd-ad
required-package: adcli
required-package: samba-common-tools
login-formats: %U@startup.company
login-policy: allow-realm-logins
devos@devserver:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:fe:73:56 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname enx00c29fe7356
    inet 192.168.10.103/24 brd 192.168.10.255 scope global dynamic noprefixroute ens160
        valid_lft 6937sec preferred_lft 6937sec
    inet6 fe80::15a9:e733:de33:58b8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
devos@devserver:~$

devos@fedora:~$ ping 192.168.10.100
PING 192.168.10.100 (192.168.10.100) 56(84) bytes of data.
64 bytes from 192.168.10.100: icmp_seq=1 ttl=128 time=0.277 ms
64 bytes from 192.168.10.100: icmp_seq=2 ttl=128 time=0.326 ms
64 bytes from 192.168.10.100: icmp_seq=3 ttl=128 time=0.306 ms
64 bytes from 192.168.10.100: icmp_seq=4 ttl=128 time=0.317 ms
^C
--- 192.168.10.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3072ms
rtt min/avg/max/mdev = 0.277/0.306/0.326/0.018 ms
devos@fedora:~$ realm list
startup.company
type: kerberos
realm-name: STARTUP.COMPANY
domain-name: startup.company
configured: kerberos-member
server-software: active-directory
client-software: sssd
required-package: sssd-common
required-package: oddjob
required-package: oddjob-mkhomedir
required-package: sssd-ad
required-package: adcli
required-package: samba-common-tools
login-formats: %U@startup.company
login-policy: allow-realm-logins
devos@fedora:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:59:25:f8 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    altname enx00c295925f8
    inet 192.168.10.102/24 brd 192.168.10.255 scope global dynamic noprefixroute ens160
        valid_lft 7099sec preferred_lft 7099sec
    inet6 fe80::3303:c360:d93b:5c3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
devos@fedora:~$
  
```



After each machine successfully joined the domain, the connected devices became visible in the DNS settings on the domain controller. They appeared along with their respective IP addresses and hostnames.

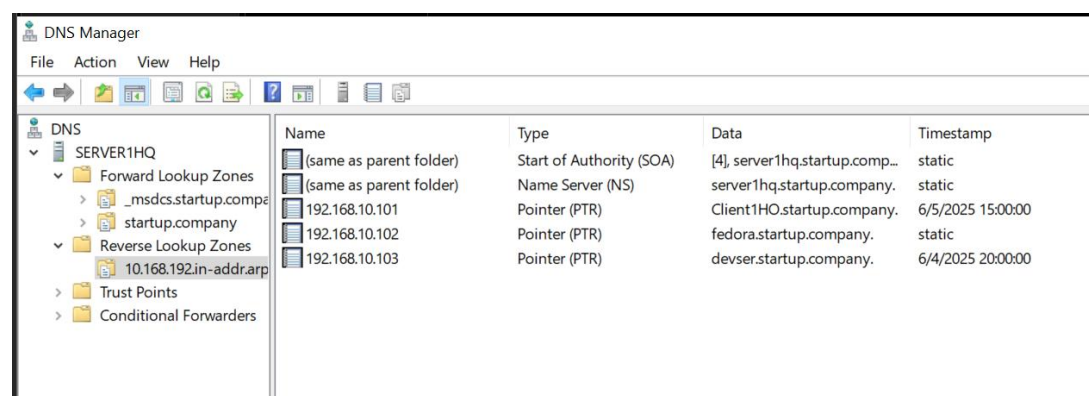


Name	Type	Data	Timestamp
_msdcs	Start of Authority (SOA)	[387], server1hq.startup.co...	static
_sites	Name Server (NS)	server1hq.startup.company.	static
_tcp	Host (A)	192.168.10.100	6/5/2025 11:00:00
_udp	Host (A)	192.168.10.101	6/5/2025 14:00:00
devser	Host (A)	192.168.10.103	6/5/2025 12:00:00
fedora	Host (A)	192.168.10.102	static
server1hq	Host (A)	192.168.10.100	static

After each machine successfully joined the domain, the connected devices became visible in the DNS settings on the domain controller. They appeared along with their respective IP addresses and hostnames, as shown in the image below.

Additionally, a reverse lookup zone was also created using the following method: by right-clicking on Reverse Lookup Zones and selecting New Zone. The Primary zone option was chosen, followed by the To all DNS servers running on domain controllers in this domain (startup.company) option. Next, the IPv4 Reverse Lookup Zone was selected. In the corresponding field, the network ID 192.168.10 was entered.

In the second-to-last step, the Allow only secure dynamic updates option was selected, and finally, the Finish button was clicked.



Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[4], server1hq.startup.comp...	static
(same as parent folder)	Name Server (NS)	server1hq.startup.company.	static
192.168.10.101	Pointer (PTR)	Client1HO.startup.company.	6/5/2025 15:00:00
192.168.10.102	Pointer (PTR)	fedora.startup.company.	static
192.168.10.103	Pointer (PTR)	devser.startup.company.	6/4/2025 20:00:00

### 3.5. Azure File Sharing and VPN Configuration

The first step was to create two Azure Storage Accounts: storagemain2025 and clientfaceoffice. Each account had one SMB file share attached — siteabc, designed for secure file sharing between sites, and sitec, intended to provide guest users with read-only access to a copy of marketing materials, thereby protecting sensitive data.

The image displays two screenshots of the Azure portal interface, showing the configuration of SMB file shares for two different storage accounts.

**Top Screenshot: sitec File Share**

- Navigation:** Home > Resource groups > StartUp > storagemain2025 | File shares > siteabc > StartUp > clientfaceoffice | File shares
- Overview:** Overview, Diagnose and solve problems, Access Control (IAM), Browse, Operations, Snapshots, Backup.
- Essentials:**
  - Storage account: clientfaceoffice
  - Resource group: StartUp
  - Location: Norway East
  - Subscription: Basic
  - Subscription ID: 1deb36de-58a1-435a-9f9a-81cbba7b3dd2
- Properties:**
  - Size:** Maximum storage (GiB): 102400, Used storage capacity (GiB): 0, Access tier: Hot.
  - Performance:** IOPS: Varies by region. Learn more, Throughput (MiB/sec): Varies by region. Learn more.
  - Backup:** Snapshots: 4 snapshots, Last modified: 5/25/2025, 9:31:06 PM.
- Feature status:**
  - Soft delete: 30 days
  - Large file shares: Enabled
- Identity-based access:** Directory service: Not configured, Domain: -
- SMB protocol settings:** Security profile: Maximum compatibility, SMB protocol versions: -, SMB channel encryption: -

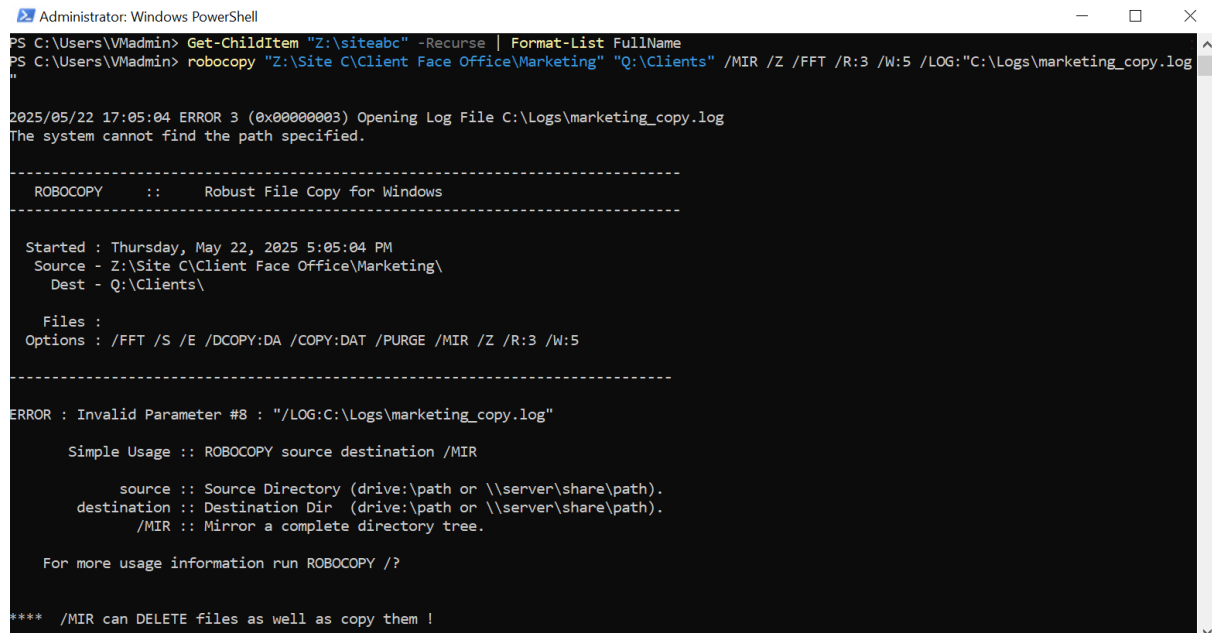
**Bottom Screenshot: siteabc File Share**

- Navigation:** Home > Resource groups > StartUp > storagemain2025 | File shares > siteabc
- Overview:** Overview, Diagnose and solve problems, Access Control (IAM), Browse, Operations, Snapshots, Backup.
- Essentials:**
  - Storage account: storagemain2025
  - Resource group: StartUp
  - Location: Norway East
  - Subscription: Basic
  - Subscription ID: 1deb36de-58a1-435a-9f9a-81cbba7b3dd2
- Properties:**
  - Size:** Maximum storage (GiB): 102400, Used storage capacity (GiB): 0, Access tier: Transaction optimized.
  - Performance:** IOPS: Varies by region. Learn more, Throughput (MiB/sec): Varies by region. Learn more.
  - Backup:** Snapshots: 0 snapshots, Last modified: -
- Feature status:**
  - Soft delete: 30 days
  - Large file shares: Enabled
- Identity-based access:** Directory service: Configured, Domain: -
- SMB protocol settings:** Security profile: Maximum compatibility, SMB protocol versions: -, SMB channel encryption: -

Next, a Windows Server was deployed, and both file shares were mounted to it. This setup was necessary, among other reasons, to connect the server to the existing corporate domain. After joining the domain, folders for the three sites were created on the siteabc share via Remote Desktop. These site folders were further divided into department-specific folders (Admin, HR, Marketing, Programming, Software Development, Sales/Client-facing Office), with access permissions assigned only to the relevant employees.

On the sitec share, a marketing folder was created with read-only permissions for guest users.

Following this, a scheduled daily copy task was configured using Robocopy and Task Scheduler to synchronize the contents of the Marketing folder from Site A to the guest marketing folder. This ensured that guests had up-to-date access to marketing materials.



```
Administrator: Windows PowerShell
PS C:\Users\VMadmin> Get-ChildItem "Z:\siteabc" -Recurse | Format-List FullName
PS C:\Users\VMadmin> robocopy "Z:\Site C\Client Face Office\Marketing" "Q:\Clients" /MIR /Z /FFT /R:3 /W:5 /LOG:"C:\Logs\marketing_copy.log"

2025/05/22 17:05:04 ERROR 3 (0x00000003) Opening Log File C:\Logs\marketing_copy.log
The system cannot find the path specified.

-----
ROBOCOPY      ::      Robust File Copy for Windows
-----

Started : Thursday, May 22, 2025 5:05:04 PM
Source - Z:\Site C\Client Face Office\Marketing\
Dest - Q:\Clients\

Files :
Options : /FFT /S /E /DCOPY:DA /COPY:DAT /PURGE /MIR /Z /R:3 /W:5

-----
ERROR : Invalid Parameter #8 : "/LOG:C:\Logs\marketing_copy.log"

Simple Usage :: ROBOCOPY source destination /MIR

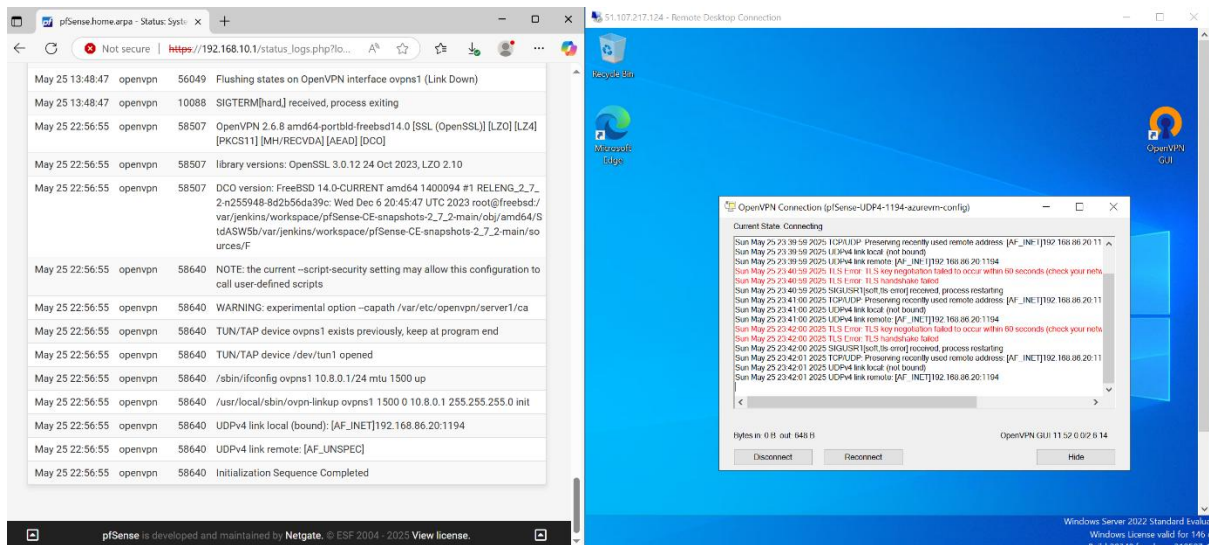
source :: Source Directory (drive:\path or \\server\share\path).
destination :: Destination Dir (drive:\path or \\server\share\path).
/MIR :: Mirror a complete directory tree.

For more usage information run ROBOCOPY /?

**** /MIR can DELETE files as well as copy them !
```

The next step involved connecting the Azure VM to a Virtual Network (VNet), which would then connect to the VPN Gateway. A GatewaySubnet was created within the VNet, a technical prerequisite for the VPN Gateway's operation. A public IP address was assigned to the VPN Gateway to enable connections from the other side.

An OpenVPN server was then configured on the PfSense firewall to connect with the Azure VPN Gateway. Phase 1 and Phase 2 policies were set up, defining encryption keys and IP ranges. The VPN configuration file was exported and transferred to the Azure VM. The OpenVPN client was launched on the VM; however, the connection failed due to a TLS error stating "TLS handshake failed."



One potential solution considered was port forwarding, but due to lack of access to the local router, this could not be implemented.

Unfortunately, at this point, I made a significant error by accidentally deleting all screenshots of the configurations and settings. Additionally, after the failed VPN attempt to connect the VMware domain to Azure, approximately 90% of the entire Azure setup was lost. I attempted to recover and reproduce the setup with new configurations, but the Azure credit of about 1000-1200 NOK had expired, so this part remained incomplete.

Afterwards, I tried to reproduce the file sharing setup locally, and the following screenshots illustrate this effort.

## 3.6. Correction, Reproduction

### A. HDD Assignment to Domain Controller

The Domain Controller for Windows Server was assigned 2 additional HDDs while powered off.

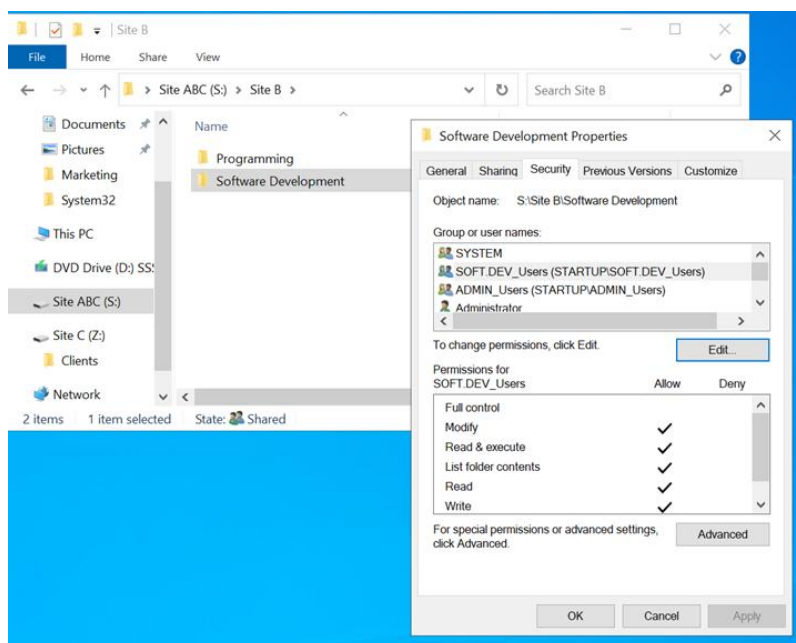
A 150 GB drive was allocated to symbolize file sharing between the three sites (Site A, B, C), consistent with the subnet ranges (e.g., 192.168.10.0/24 for Site A).

A 60 GB drive was dedicated to serving guests, copying Marketing materials from the Site ABC drive.

### B. Folder Structure and Permissions

After creating the drives, I created a folder for each site (Site A, B, C) on the Site ABC drive.

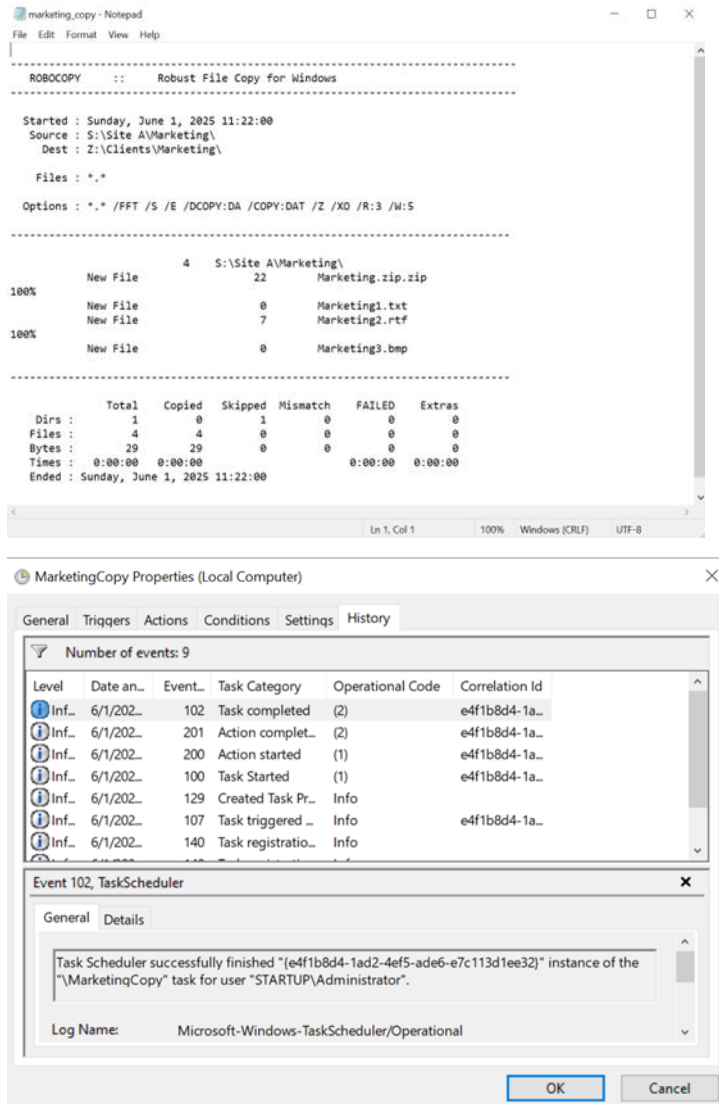
Within these folders, subfolders were made for each department, with specific access rights: only admins have full access, while others are restricted to their own department's folder for security reasons.

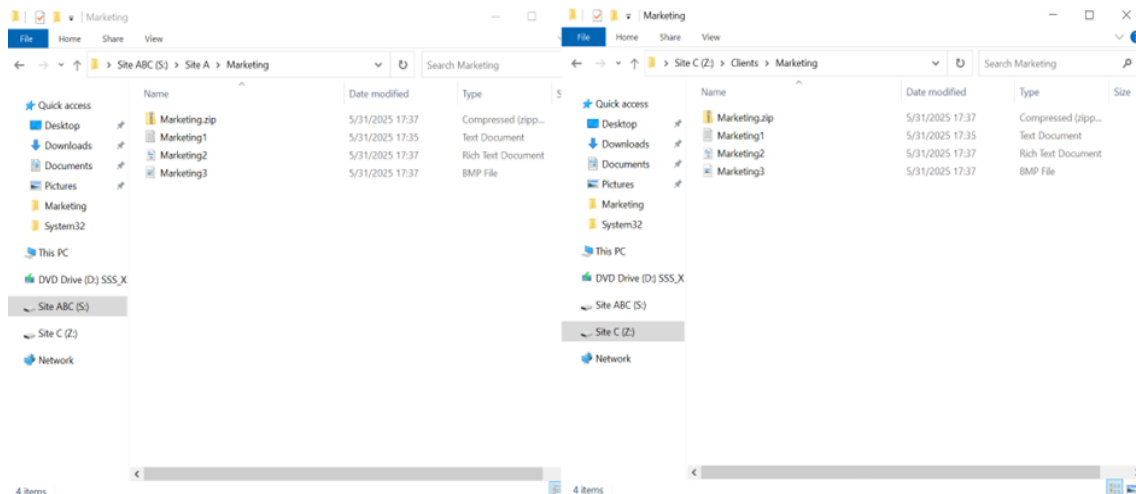
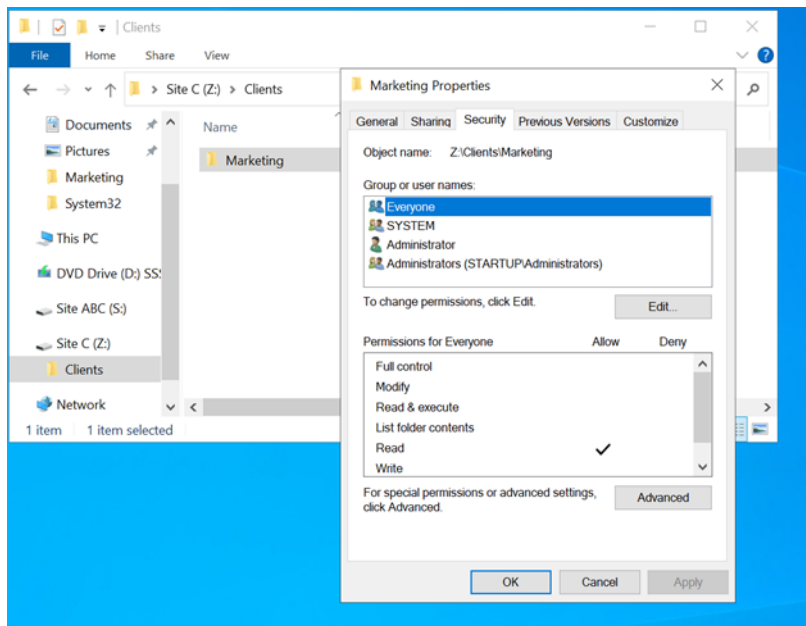


## C. Marketing Materials Copying

On the second drive, a Clients\Marketing folder was created on Site C, where Marketing materials are copied daily from the Site ABC – Site A folder for updates.

This copying is automated using Robocopy and scheduled via Task Scheduler.





## D. SMB Sharing of Site ABC Drive

In PowerShell, I selected and shared the Site ABC drive via SMB, assigning it a new drive name.

In File Explorer, I navigated to the Network tab, right-clicked the shared drive, enabled "Reconnect at sign-in," and clicked Finish.

## E. Guest Access Demonstration

To show how a guest would access the Marketing folder, I activated the guest user on the Domain Controller.

I shared the second drive via SMB with read-only permissions for everyone.

In File Explorer, I selected the Network tab, chose the drive letter V, and entered the drive's location.

On the shared drive, I right-clicked, went to the Permissions tab, selected Security, and added the guest user and "everyone" user with read-only access (full admin rights remained).

































I added all other departments with deny permissions to restrict access.

## F. PfSense VLAN70 Configuration

I connected a new network card to PfSense and configured it as VLAN70 to replicate the guest network.

I applied rules to make the domain invisible to the guest network and vice versa, preventing mutual access (e.g., denying traffic to 192.168.10.0/24 and 192.168.20.0/24).

This setup mimics a guest accessing the folder via a store Wi-Fi.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 32/139 KiB	IPv4 *	VLAN70 subnets	*	*	*	*	none		Allow full internet for guest	   
<input type="checkbox"/>	✗ 0/371 KiB	IPv4 *	VLAN70 subnets	*	*	*	*	none		Catch-all	   
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	VLAN70 subnets	*	VLAN70 subnets	*	*	none		Peer-to-Peer block	   
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	VLAN70 subnets	*	LAN address	*	*	none		VLAN 10,20,30,40,50,60 block	   
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	VLAN70 address	*	192.168.10.0/24	*	*	none			   
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	VLAN70 subnets	*	*	80 - 443	*	none		Allow web	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	VLAN70 subnets	*	*	53 (DNS)	*	none		Allow DNS	   
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	VLAN70 subnets	*	WAN subnets	445 (MS DS)	*	none		Azure File Share SMB access	   



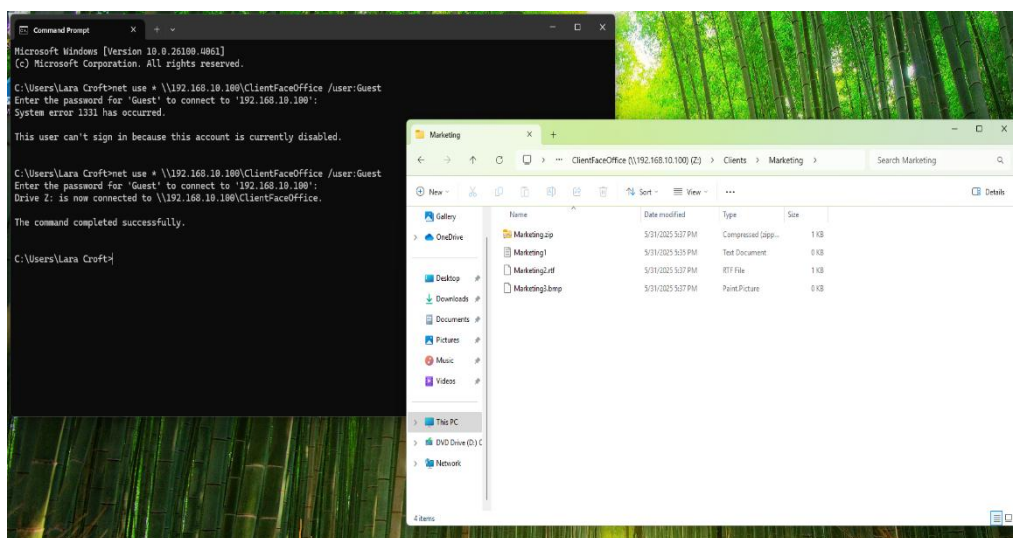
## G. Guest VM Setup and Access

I connected a new VM to the VLAN70 NIC and installed a fresh Windows 10 OS, without naming or joining it to the domain.

I opened the command prompt typed the following command:

```
net use * \\192.168.10.100\ClientFaceOffice /user:Guest
```

In File Explorer, I right-clicked the Network tab, selected drive letter Z, and entered the server's IP (192.168.10.100) and the exact share location, gaining read-only access to the Marketing materials.



### 3.7. Mounting SMB File Share on Linux Machines

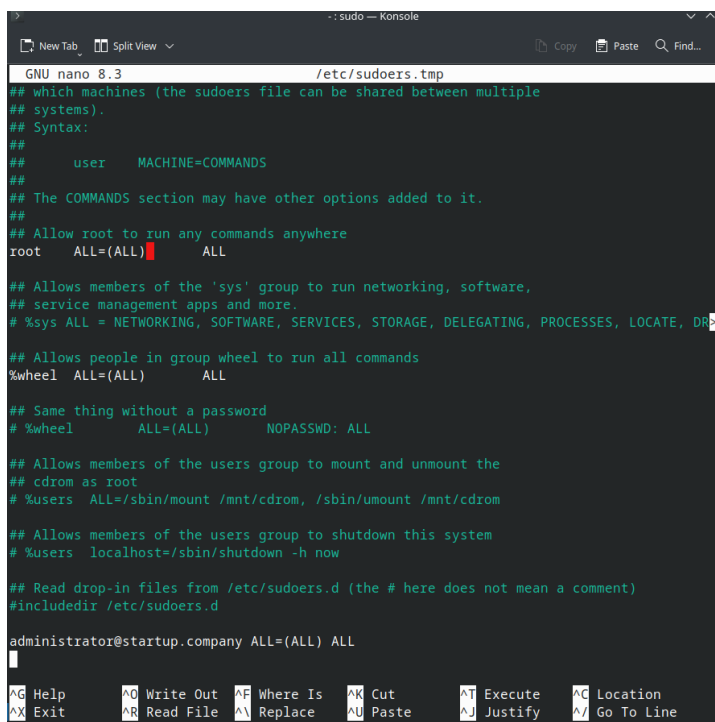
*(For security reasons, the original password has been replaced in this document with password666.)*

#### A. Integrating Permissions on Fedora Machine

As the first step, I logged into the Fedora machine using the local (root) account.

Then I opened the sudoers file using the visudo editor: *sudo visudo*

I navigated to the very bottom of the file (just below the line `#includedir /etc/sudoers.d`) and added the following line: *administrator@startup.company ALL=(ALL) ALL*



```
GNU nano 8.3 /etc/sudoers.tmp
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
## user MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root ALL=(ALL) ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DP
#

## Allows people in group wheel to run all commands
%wheel ALL=(ALL) ALL

## Same thing without a password
# %wheel ALL=(ALL) NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#include:: /etc/sudoers.d

administrator@startup.company ALL=(ALL) ALL
```

This step granted root-level (sudo) access to the domain administrator. I then saved the changes with Ctrl+O and exited using Ctrl+X.

***su - administrator@startup.company***

***sudo whoami***

***root***

```
devod@fedora:~$ sudo visudo
[sudo] password for devod:
devod@fedora:~$ su - administrator@startup.company
Password:
Last login: Sun Jun  8 10:48:16 CEST 2025 on pts/1
administrator@startup.company@fedora:~$ sudo whoami
[sudo] password for administrator@startup.company:
root
```

This confirms that administrator@startup.company now has sudo privileges on the Fedora Workstation, enabling it to mount the previously created SMB file share from the domain controller.

## B. Preparing for Mount and One-Time Mount Operation

First, I installed the required package: ***sudo dnf install cifs-utils***.

```
administrator@startup.company@fedora:~$ sudo dnf install cifs-utils
Updating and loading repositories:
Repositories loaded.
Package "cifs-utils-7.2-1.fc42.x86_64" is already installed.
Nothing to do.
```

Then, I created a mount point: ***sudo mkdir -p /mnt/startupcompany***.

After that, I mounted the share: ***sudo mount -t cifs //Server1HQ/StartupCompany /mnt/startupcompany -o username=administrator,domain=startup.company***.

```
administrator@startup.company@fedora:~$ sudo mkdir -p /mnt/startupcompany
administrator@startup.company@fedora:~$ sudo mount -t cifs //Server1HQ/StartupCompany /mnt/startupcompany -o username=administrator,domain=startup.company
Password for administrator@//Server1HQ/StartupCompany:
administrator@startup.company@fedora:~$ df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/nvme0n1p3             19G       5.1G   14G  28% /
devtmpfs                   4.0M         0  4.0M   0% /dev
tmpfs                      1.9G       12K   1.9G   1% /dev/shm
tmpfs                      772M       1.8M   770M   1% /run
tmpfs                      1.0M         0    1.0M   0% /run/credentials/systemd-journald.service
tmpfs                      1.9G       8.0K   1.9G   1% /tmp
/dev/nvme0n1p3             19G       5.1G   14G  28% /home
/dev/nvme0n1p2             974M      330M   577M  37% /boot
tmpfs                      1.0M         0    1.0M   0% /run/credentials/systemd-resolved.service
tmpfs                      386M      120K   386M   1% /run/user/1000
tmpfs                      386M       76K   386M   1% /run/user/63400500
//Server1HQ/StartupCompany 150G       98M   150G   1% /mnt/startupcompany
```

To verify, I used: ***df -h***

The output confirmed the mounted share: `//Server1HQ/StartupCompany`.

### **C. Persistent Mount via /etc/fstab**

I edited the `/etc/fstab` file: ***sudo nano /etc/fstab***

I added the following line: `/Server1HQ/StartupCompany /mnt/startupcompany cifs  
username=administrator,password=password666,domain=startup.company,uid=0,gid=0,file_mode=0755,dir_mode=0755 0 0`

To enhance security, I created a credential file: ***sudo nano /root/.smbcredentials***

Content of the file:

***username=administrator  
password=password666  
domain=startup.company***

Saved with Ctrl+O, exited with Ctrl+X.

Then I secured the credential file: ***sudo chmod 600 /root/.smbcredentials***

```
administrator@startup.company@fedora:~$ sudo nano /etc/fstab
administrator@startup.company@fedora:~$ sudo nano /root/.smbcredentials
administrator@startup.company@fedora:~$ sudo chmod 600 /root/.smbcredentials
```

I updated the `/etc/fstab` entry: `/Server1HQ/StartupCompany /mnt/startupcompany cifs  
credentials=/root/.smbcredentials,uid=0,gid=0,file_mode=0755,dir_mode=0755 0 0`

To test the setup, I ran: ***sudo mount -a***

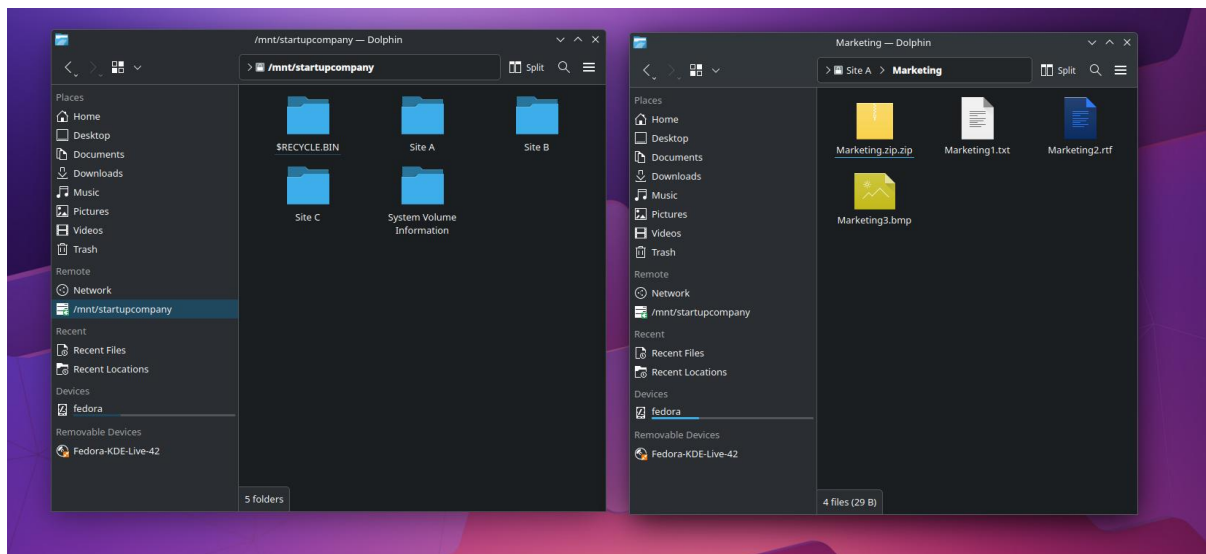
No errors occurred, confirming that the persistent mount was successful.

## D. Verification and Usage

To verify access to the mounted share: *ls -l /mnt/startupcompany*

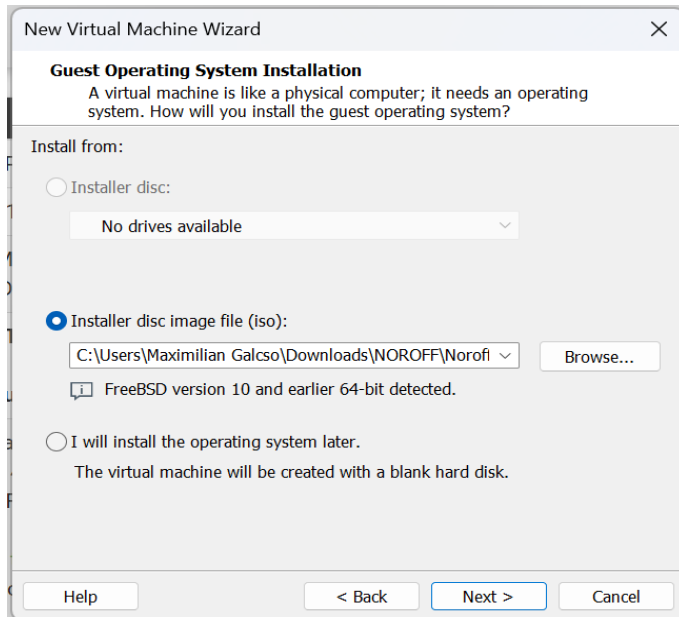
```
administrator@startup.company@fedora:~$ sudo mount -a
administrator@startup.company@fedora:~$ ls -l /mnt/startupcompany
total 0
drwxr-xr-x  2 root root 0 May 30 20:06 '$RECYCLE.BIN'
drwxr-xr-x  2 root root 0 May 31 17:45 'Site A'
drwxr-xr-x  2 root root 0 May 31 17:32 'Site B'
drwxr-xr-x  2 root root 0 May 31 17:34 'Site C'
drwxr-xr-x. 2 root root 0 Jun  1 10:56 'System Volume Information'
```

The command listed the expected directories and files from the SMB share.

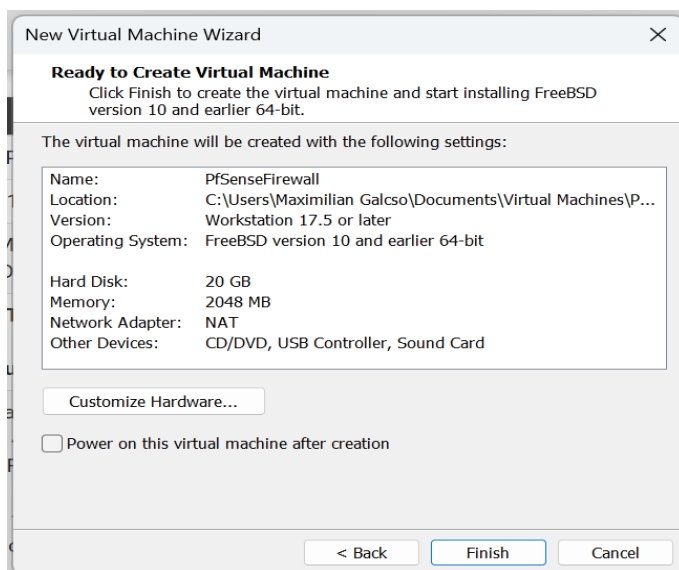


### 3.8. PfSense Firewall Installation and Configuration

In VMware Workstation, I created a new virtual machine using the latest version. During the setup process, I added the previously downloaded Netgate (PfSense) installation ISO file, named the VM, and selected the installation location. I left the default processor configuration, assigned 2 GB of RAM, and selected the NAT option for network connection mode. For disk space, I kept the default 20 GB and chose to store the virtual disk as a single file.

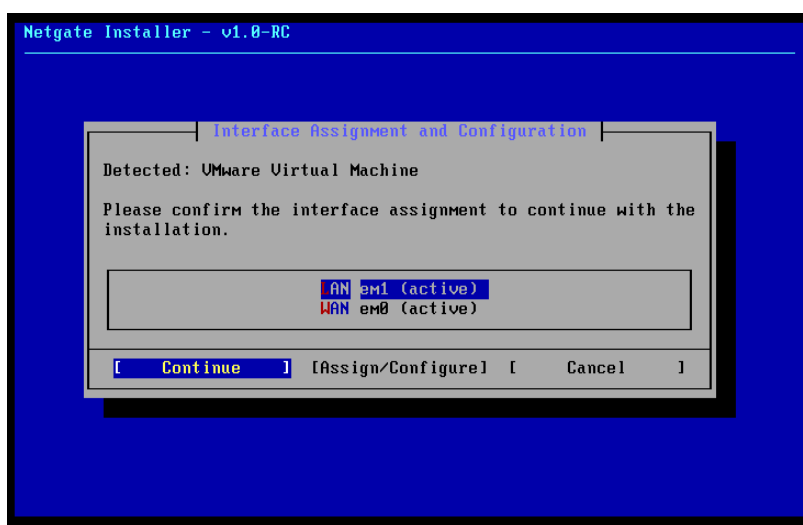
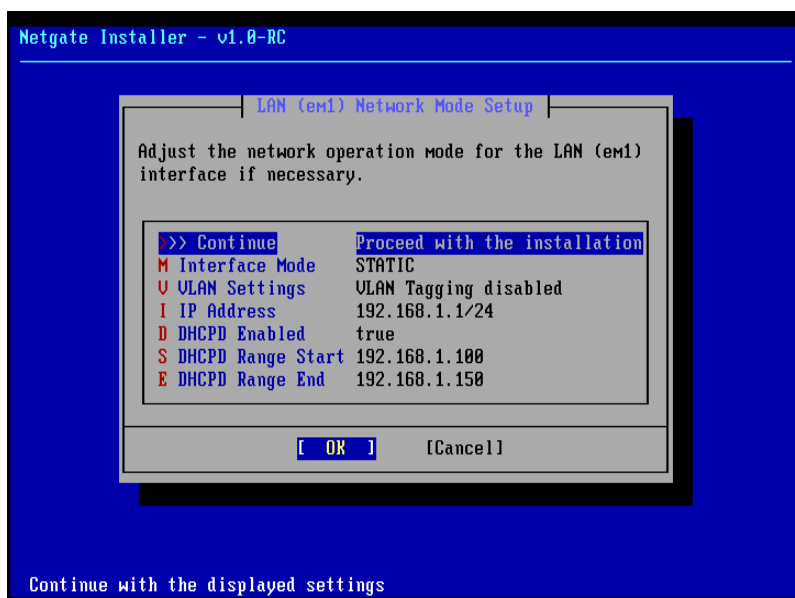


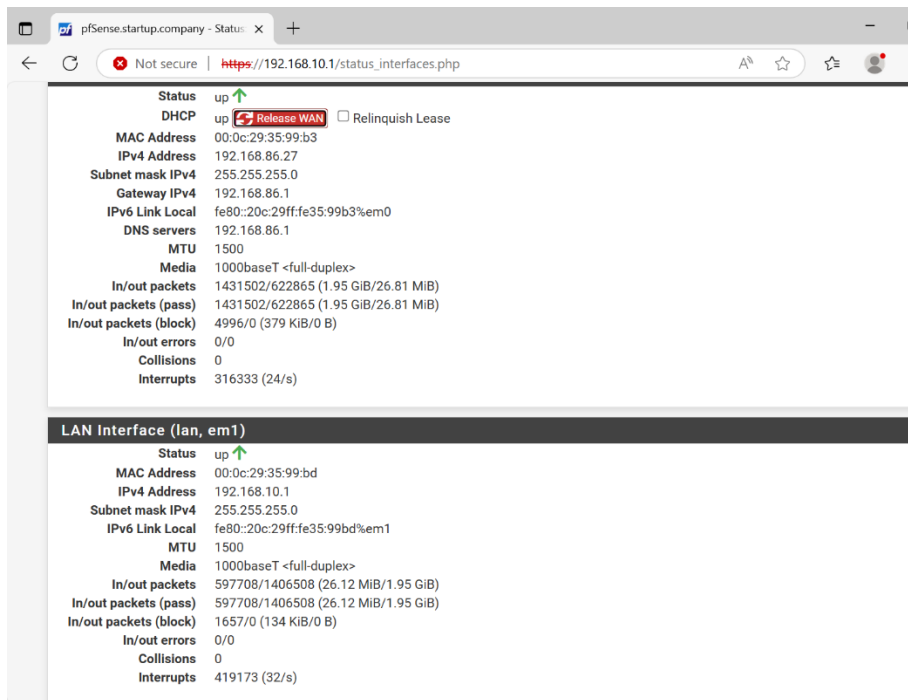
Before finishing the setup, I double-checked all settings and then clicked the Finish button to complete the VM creation.



Before starting the installation, I added a new custom network in VMware named VMnet7 and disabled DHCP for it. I then added this network adapter to the PfSense VM and changed the primary NIC to Bridged Mode. After booting the virtual machine, I proceeded with the installation of PfSense.

During the installation process, both NICs were configured and received IP addresses. The primary NIC became the WAN interface, receiving internet access for the firewall, while the secondary NIC was assigned as the LAN interface. I configured a DHCP scope for the LAN side.





Once installation was complete, I connected all previously installed virtual machines (Fedora Server, Fedora Workstation, Windows Server 2022, and Windows 10) to the firewall by changing their network adapters to VMnet7, ensuring that all machines now receive internet access and dynamic IP addresses via the PfSense firewall.

Next, I created another custom VMnet in VMware, set to NAT mode, and added this as a third NIC to the PfSense VM. I then connected a guest Windows client to this new VMnet, changing its mode to Host-Only in an attempt to simulate a scenario where the guest user connects via Wi-Fi (as if from a shop or public network) and accesses the shared folder through a restricted and isolated environment.



## **4. Limitations, Conclusions, and Recommendations**

### **4.1. What I Learned During the Project**

Throughout this hybrid IT infrastructure project, I gained a vast amount of knowledge, both technical and practical. Perhaps the most important lesson was learning how to plan and gradually build a complex system—even in a simulated environment. I deepened my understanding of VLAN segmentation, firewall configuration, Active Directory operations, and hybrid file sharing using Azure.

Before this, I had never built a network that integrates multiple operating systems (Windows Server, Windows 10, Fedora) and separates them securely through a common firewall. I also had no prior hands-on experience in synchronizing cloud storage with local infrastructure or managing file access based on role-based permissions across departments.

One of the key takeaways was that having a working system is not enough—it must also be secure, transparent, cost-efficient, and sustainable in the long term. This shift in mindset had a significant impact on me, and I intend to carry it into my future work.

### **4.2. New Tools and Technical Challenges**

This project allowed me to explore many new tools and concepts. I applied knowledge not only from this course but also from external platforms such as HackTheBox and TryHackMe—whether in organizing Active Directory users or implementing appropriate protocols and rules. One of the most significant experiences was the complete utilization of the PfSense firewall. Previously, I had only read about it, but this time I configured real traffic control, NAT, VLAN segmentation, and DHCP through it.

A particularly interesting challenge was setting up the guest network (VLAN70), where I wanted to grant read-only access to a shared folder while blocking all other traffic.

Using Azure cloud storage was also new to me—especially the part about permission management and integrating it with a local network environment. Although I couldn't fully implement Azure AD due to limitations, I successfully simulated a scenario in which the sales department at one site could access marketing materials stored remotely.

### 4.3. What Went Smoothly and What Caused Difficulty

Some parts of the project went smoother than I expected. Windows Server 2022 turned out to be surprisingly stable, and configuring AD, DNS, and GPOs didn't present any major difficulties.

This was likely because I had spent more time on this subject than on others, and when I got stuck, I had the opportunity to ask for advice and support from knowledgeable people like **Marco Hoyvang** or **Kjetil Andre**. That's partly why I switched to this project topic in the first place.

My teacher, **Chantal Van Wyk**, played a significant role by offering encouraging words and praise throughout the project, which greatly boosted my motivation and attitude. Looking back, I realize that better time structuring and earlier testing could have reduced stress and improved clarity. This experience, along with Chantal's support, is a valuable lesson for my future professional projects.

However, I did face some serious challenges in certain areas:

- **PfSense firewall rules:** I had to rework my approach several times to ensure the system was both secure and usable—especially in the guest VLAN, where access had to be limited to just one specific share.
- **VPN implementation:** I initially planned to include a VPN to simulate remote access. Unfortunately, I couldn't finalize this due to issues with PfSense configuration and certificate management. Instead, I used a NAT-based Host-Only network to simulate guest access.
- **Cloud integration:** Full Azure AD hybrid identity management was not achievable in this environment, so I only implemented partial simulation through file sharing and access control.
- **Documentation:** Arguably the hardest part of the project. I'm not used to writing down what I do, describing my work, or capturing screenshots. I tend to operate on instinct or routine, which often leads to mistakes. I usually focus more on action than on communication—whether verbal or written.

#### 4.4. Reflection and Self-Evaluation

My original goal was to build a secure, well-segmented, hybrid IT infrastructure for a multi-site company divided into departments—something that would be viable in 2025, even from an environmental perspective, anywhere in the world. The main objectives were:

- Department-specific VLANs
- Firewall-based traffic control and guest access limitation
- Active Directory and group-based permission management
- Integration of Linux and Windows systems
- Simulation of cloud-based file sharing
- Guest access over Wi-Fi with restricted permissions

Although I couldn't fully implement every part, I met most of the goals. The system works, is secure, and reflects real-world practices.

I'm particularly proud of how I managed role-based file access using GPOs, and how traffic control through PfSense created a secure foundation for VLAN isolation.

One of the biggest lessons from the project for me was that effective time management is crucial in designing and implementing complex systems. Although I developed the concept relatively early, breaking down subtasks and testing practical configurations often took more time than I initially anticipated. This was especially true for parts where I had to learn new technologies—such as joining Fedora machines to a domain or fine-tuning PfSense. Looking back, I feel that if I had structured my time better and started testing the components earlier, I could have worked with less stress and greater clarity. This is an important lesson that will serve me well in my future professional projects.

## 4.5. Future Improvements and Recommendations

If I were to restart or further develop this project, I would do the following differently:

- **Start with the firewall:** After designing the topology, I would add one network adapter per VLAN and configure them immediately. As it stands, the current setup turned out to be quite chaotic—possibly why not everything worked smoothly.
- **Set up all VLANs first,** then add devices to their designated VLANs one by one.
- **Be more patient and plan more carefully.** I had many new ideas along the way, and I kept trying to implement them, which sometimes disrupted earlier progress.
- **Leave cloud integration (Azure) for last,** after all local systems are properly set up.
- **Implement a complete VPN solution:** Using OpenVPN or WireGuard, I could enable secure remote access for authenticated users.
- **Use real networking equipment:** A physical switch with VLAN support would make the simulation more realistic.
- **Centralized logging:** It would be ideal to collect logs from PfSense and servers in one place using a syslog or cloud-based solution.
- **Azure AD integration:** In a production environment, using Azure AD Connect to link on-prem AD with Azure would give better identity and access control.

## 4.6. Final Thoughts

This project was more than just an exam assignment—it was a real challenge that tested my technical knowledge, design skills, troubleshooting ability, documentation habits, and personal patience. I didn't just learn how to build a hybrid IT system—I learned how to think in terms of systems and long-term planning.

I also realized how important proper documentation is—screenshots and written records alike. I lacked images in some sections, which forced me to redo parts and resulted in doing the same work multiple times.

Some parts of the project turned out well, others less so, but I learned from every step. I now have a deeper understanding of network segmentation, layered security, and permission management.

Overall, I believe I met most of my initial goals, and I created a working, documented, and demonstrable system. I'm proud of what I built—even though not everything turned out the way I originally envisioned. I'm confident that I will be able to design even better infrastructures in the future.

## Bibliography

Academy.hackthebox.com (2025) HackTheBox Academy. Available at: <https://academy.hackthebox.com/sso/redirect> (Accessed: June 8, 2025).

App.hackthebox.com (2025) HackTheBox LAB. Available at: <https://app.hackthebox.com/sso/redirect> (Accessed: June 8, 2025).

Broadcom Inc. (2025) How to create virtual machines in VMware Workstation 17 Pro. Available at: <https://knowledge.broadcom.com/external/article/315434/how-to-create-virtual-machines-in-vmware.html> (Accessed: June 8, 2025).

Fedoramagazine.org (2024) Join Fedora Linux to an enterprise domain. Available at: <https://fedoramagazine.org/join-fedora-linux-enterprise-domain/> (Accessed: June 8, 2025).

Fedoraproject.org (2025) Adding a user to the sudoers file. Available at: [https://docs.fedoraproject.org/en-US/quick-docs/adding\\_user\\_to\\_sudoers\\_file/](https://docs.fedoraproject.org/en-US/quick-docs/adding_user_to_sudoers_file/) (Accessed: June 8, 2025).

Fedoraproject.org (2025) Fedora Project. Available at: <https://fedoraproject.org/> (Accessed: June 8, 2025).

Forbes.com (2019) How a hybrid server can give you the best of both worlds. Available at: <https://www.forbes.com/councils/forbestechcouncil/2019/06/20/how-a-hybrid-server-can-give-you-the-best-of-both-worlds/> (Accessed: June 8, 2025).

Hostwinds.com (2025) How to map your Windows server drive as a network drive. Available at: <https://www.hostwinds.com/tutorials/how-to-map-your-windows-server-drive-as-a-network-drive> (Accessed: June 8, 2025).

Lazyadmin.nl (2025) Robocopy ultimate guide. Available at: <https://lazyadmin.nl/it/robocopy-ultimate-guide/> (Accessed: June 8, 2025).

Microsoft.com (2025) Evaluation Center. Available at: <https://www.microsoft.com/en-us/evalcenter/> (Accessed: June 8, 2025).

Microsoft.com (2025) How to enable Active Directory Domain Services (AD DS) authentication in Azure Files. Available at: <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-ad-ds-enable> (Accessed: June 8, 2025).

Microsoft.com (2025) Hybrid cloud considerations. Available at: <https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/hybrid-considerations> (Accessed: June 8, 2025).

Microsoft.com (2025) Install Active Directory Domain Services (Level 100). Available at: <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-> (Accessed: June 8, 2025).

Netgate.com (2025) Example basic configuration for pfSense software. Available at: <https://docs.netgate.com/pfsense/en/latest/recipes/example-basic-configuration.html> (Accessed: June 8, 2025).

Pfsense.org (2025) pfSense: Open Source Network Firewall and VPN. Available at: <https://www.pfsense.org/> (Accessed: June 8, 2025).

Redhat.com (2025) Mounting SMB shares. Available at: [https://docs.redhat.com/en/documentation/red\\_hat\\_enterprise\\_linux/9/html/managing\\_file\\_systems/mounting-file-systems\\_managing-file-systems#mounting-smb-shares\\_managing-file-systems](https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/managing_file_systems/mounting-file-systems_managing-file-systems#mounting-smb-shares_managing-file-systems) (Accessed: June 8, 2025).

Research.aimultiple.com (2025) Hybrid IT infrastructure in 2025: Benefits & challenges. Available at: <https://research.aimultiple.com/hybrid-it-infrastructure/> (Accessed: June 8, 2025).

Tryhackme.com (2025) Cyber Security 101 Path. Available at: <https://tryhackme.com> (Accessed: June 8, 2025).

Ubuntu.com (2020) mount.cifs(8) - Linux man page. Available at: <https://manpages.ubuntu.com/manpages/focal/man8/mount.cifs.8.html> (Accessed: June 8, 2025).

Woshub.com (2025) Mapping network drives and shared folders with Group Policy (GPO). Available at: <https://woshub.com/map-network-drives-shared-folders-gpo/> (Accessed: June 8, 2025).