Rapport E6

BTS SIO - Option SISR

Mise en place d'une infrastructure réseau virtualisée

Nom : Bouhassoun
Prénom : Ilyas
Établissement : MyDigitalSchool / ESICAD
Année : 2025-2026

Table des matières

Chapitre 1

Introduction

1.1 Contexte du projet

Dans le cadre de ma formation en BTS SIO option SISR (Solutions d'Infrastructure, Systèmes et Réseaux), j'ai été amené à concevoir et mettre en place une infrastructure réseau virtualisée simulant un environnement d'entreprise.

Ce projet s'inscrit dans une démarche professionnelle visant à reproduire les besoins réels d'une organisation en matière de gestion des utilisateurs, de sécurisation du réseau et d'administration centralisée.

Pour cela, une infrastructure a été déployée sur un environnement de virtualisation (Proxmox), permettant la création de plusieurs machines virtuelles représentant les différents services de l'entreprise.

L'architecture mise en place comprend un pare-feu avec pfSense afin de sécuriser et contrôler les flux réseau, un serveur Windows configuré en contrôleur de domaine avec Active Directory pour la gestion centralisée des utilisateurs et des ressources, ainsi que plusieurs postes clients intégrés au domaine représentant différents services de l'entreprise.

Une organisation logique a également été mise en place à l'aide d'unités d'organisation (OU) et de stratégies de groupe (GPO).

Ce projet a pour objectif de mettre en œuvre des compétences liées à la conception et à l'administration d'un réseau, à la gestion des identités et des accès, à la sécurisation des échanges réseau ainsi qu'à l'automatisation de la configuration des postes.

1.2 Problématique

Dans un contexte d'entreprise, la gestion des utilisateurs, des postes de travail et la sécurisation des échanges réseau représentent des enjeux majeurs. Il est donc essentiel de mettre en place une infrastructure réseau centralisée, sécurisée et facilement administrable.

La problématique de ce projet est la suivante : comment concevoir une infrastructure permettant de gérer efficacement les utilisateurs, les ressources et les flux réseau ?

Pour répondre à cette problématique, plusieurs éléments doivent être pris en compte, notamment la centralisation des comptes utilisateurs, la sécurisation du réseau à l'aide d'un pare-feu, l'organisation des postes de travail selon les services de l'entreprise, ainsi que la mise en place d'outils facilitant l'administration.

1.3 Objectifs

L'objectif de ce projet est de concevoir et déployer une infrastructure réseau virtualisée simulant un environnement d'entreprise.

Pour répondre à cette problématique, plusieurs objectifs ont été définis :

Objectif principal

Mettre en place une infrastructure réseau fonctionnelle, sécurisée et administrable.

Objectifs spécifiques

Installer un environnement de virtualisation. Mettre en place un pare-feu pfSense. Déployer un serveur Windows avec Active Directory. Créer des OU (Compta, RH, IT). Configurer des GPO. Intégrer des postes clients au domaine. Tester le fonctionnement du réseau.

1.4 Architecture réseau

Description de l'architecture réseau du projet :

A COMPLETER

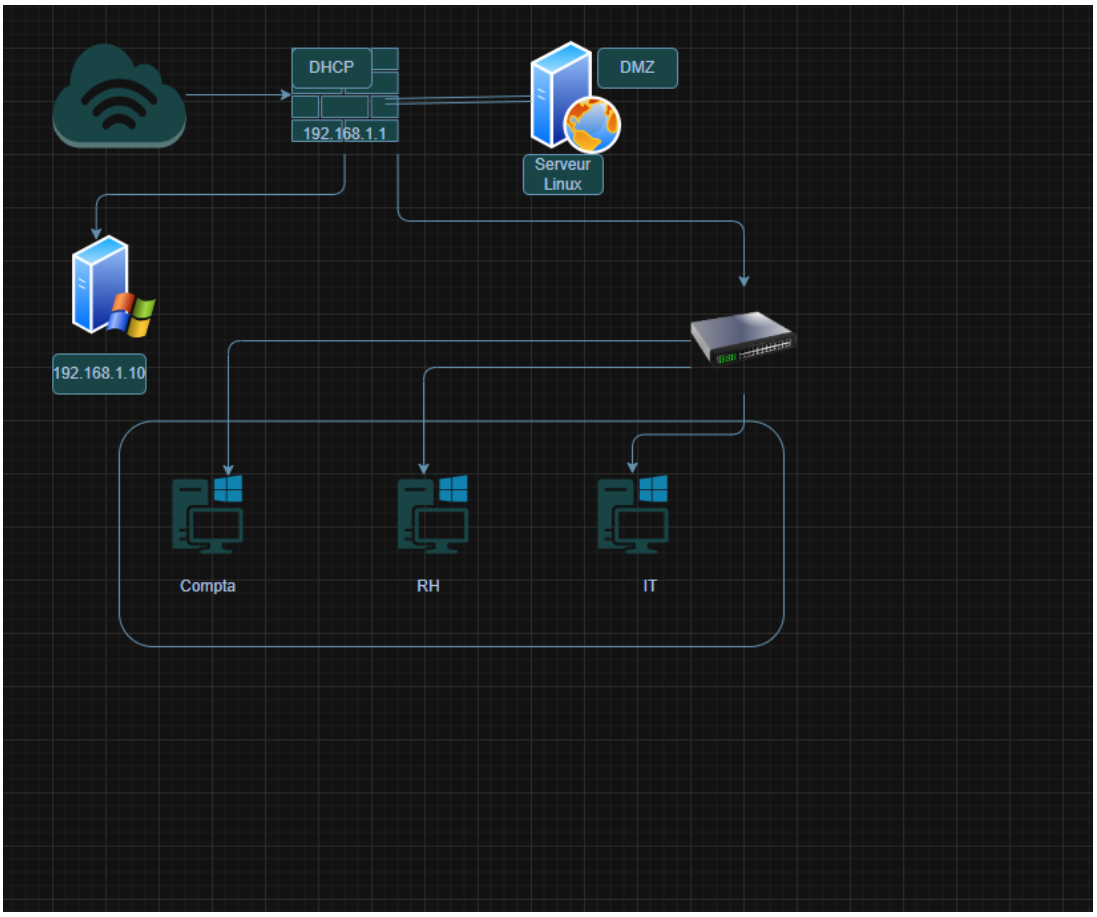

FIGURE 1.1 – Schéma de l'architecture réseau

Chapitre 2

Accès à l'infrastructure

2.1 Connexion au VPN

Afin d'accéder à l'environnement de travail distant, une connexion VPN a été mise en place. Cette connexion permet de sécuriser les échanges entre le poste client et l'infrastructure hébergée sur le serveur de virtualisation.

La connexion VPN permet d'intégrer le poste de travail dans le réseau de l'établissement comme s'il était en local, offrant ainsi un accès aux ressources internes telles que les machines virtuelles et les services réseau.

Étapes de connexion :

— Récupération des identifiants VPN fournis par l'établissement
— Lancement du client VPN sur le poste de travail
— Saisie des identifiants de connexion
— Établissement du tunnel sécurisé vers le réseau distant

Une fois connecté, il est possible d'accéder à l'interface de gestion du serveur de virtualisation Proxmox VE via un navigateur web.

Cette étape est essentielle car elle permet de gérer les machines virtuelles à distance et de réaliser l'ensemble des configurations nécessaires au projet.

Sécurité :

L'utilisation du VPN garantit la confidentialité et l'intégrité des données échangées grâce au chiffrement des communications entre le client et le réseau distant.

2.2 Accès à Proxmox

Accès à l'interface de virtualisation.

Une fois la connexion VPN établie, l'accès à l'interface de gestion de l'infrastructure est réalisé via un navigateur web.

L'interface du serveur de virtualisation Proxmox VE est accessible en saisissant l'adresse IP du serveur suivie du port de gestion.

L'utilisateur doit ensuite s'authentifier à l'aide de ses identifiants afin d'accéder à l'environnement de virtualisation.

Cette interface permet de :

— créer et gérer les machines virtuelles ;
— configurer les ressources (CPU, RAM, stockage) ;
— administrer le réseau virtuel.

Cette étape constitue le point d'entrée principal pour la mise en œuvre de l'infrastructure

du projet.

2.3 Création des machines virtuelles

Création des machines virtuelles.

Dans le cadre de ce projet, plusieurs machines virtuelles ont été créées afin de simuler une infrastructure réseau d'entreprise.

Ces machines ont été déployées à l'aide de l'hyperviseur Proxmox VE, permettant de gérer efficacement les ressources matérielles et de virtualiser différents systèmes d'exploitation.

Objectif.

L'objectif est de reproduire un environnement réaliste comprenant un pare-feu, un serveur, des postes clients ainsi qu'une zone démilitarisée (DMZ), chacun ayant un rôle spécifique dans l'infrastructure.

Machines mises en place.

Les machines suivantes ont été créées :

Un pare-feu avec pfSense pour gérer et sécuriser les flux réseau. Un serveur Windows configuré en contrôleur de domaine (Active Directory). Plusieurs postes clients Windows (Comptabilité, Ressources Humaines, Informatique). Un serveur Linux placé dans une DMZ afin d'isoler certains services du réseau interne.

Paramètres généraux.

Chaque machine virtuelle a été configurée avec des ressources adaptées :

Allocation de mémoire (RAM). Nombre de processeurs (CPU). Espace de stockage. Configuration réseau (cartes réseau virtuelles).

Ces paramètres ont été définis en fonction du rôle de chaque machine afin d'assurer un fonctionnement optimal de l'ensemble de l'infrastructure.

Intérêt de la virtualisation :

L'utilisation de la virtualisation permet :

Une meilleure gestion des ressources. Une isolation des machines. Une flexibilité dans le déploiement et les tests. La mise en place d'une architecture incluant une DMZ pour renforcer la sécurité. Une reproduction d'un environnement professionnel à moindre coût.

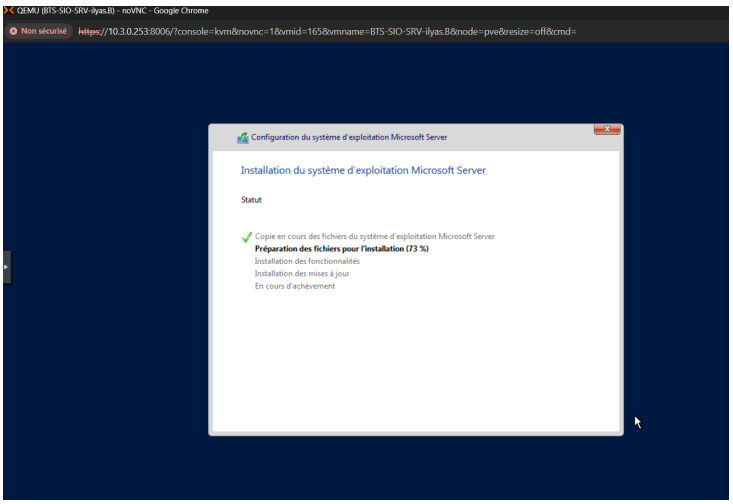

FIGURE 2.1 – Installation du serveur

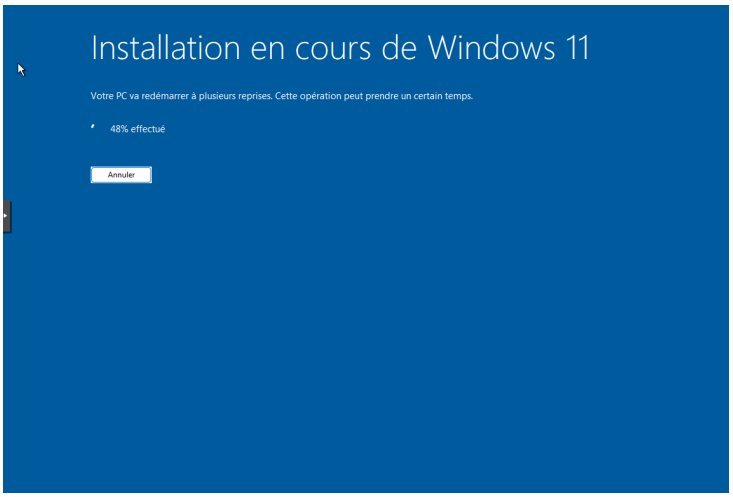

FIGURE 2.2 – Installation de Windows

Chapitre 3

Création du réseau virtuel

3.1 Création des cartes réseau

Dans le cadre de la mise en place de l'infrastructure, plusieurs cartes réseau virtuelles ont été créées afin de segmenter le réseau et d'assurer une communication structurée entre les différentes machines.

Ces cartes réseau ont été configurées sur l'hyperviseur Proxmox VE sous forme de bridges réseau.

Objectif.

L'objectif est de séparer les différents flux réseau en créant plusieurs zones :

Un réseau WAN simulant l'accès à Internet. Un réseau LAN correspondant au réseau interne de l'entreprise. Un réseau DMZ permettant d'isoler les services exposés.

Configuration mise en place.

Trois interfaces réseau ont été définies :

Une interface WAN connectée au réseau externe. Une interface LAN pour les machines internes (serveur, postes clients). Une interface DMZ pour isoler le serveur Linux.

Chaque machine virtuelle a été associée à une ou plusieurs cartes réseau en fonction de son rôle dans l'infrastructure.

Intérêt.

Cette segmentation permet :

Une meilleure organisation du réseau. Une isolation des services sensibles. Un renforcement de la sécurité grâce à la séparation des zones.

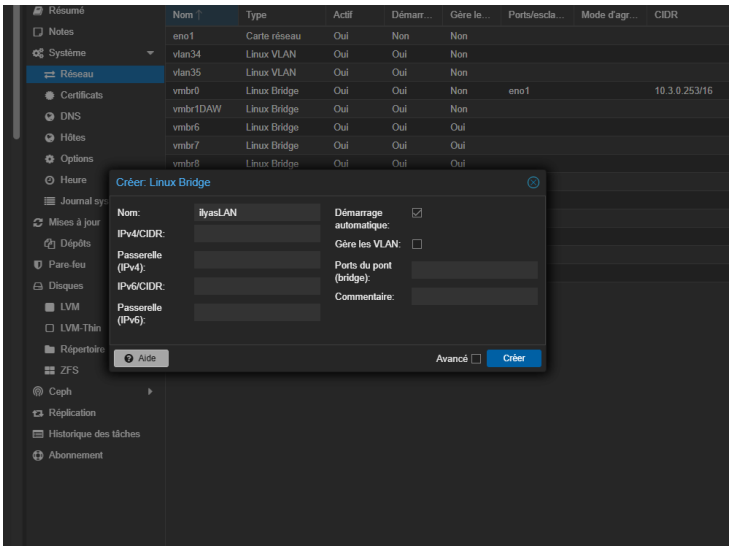

FIGURE 3.1 – Création de la carte

Chapitre 4

Installation et configuration de pfSense

4.1 Configuration des interfaces

Configuration des interfaces réseau.

Après l'installation, les interfaces réseau de pfSense ont été configurées afin de structurer l'architecture réseau en plusieurs zones.

Interfaces mises en place.

Trois interfaces principales ont été définies :

— WAN : connectée au réseau externe (accès Internet)

— LAN : réseau interne de l'entreprise

— DMZ : zone isolée destinée à héberger des services exposés

Chaque interface a été associée à une carte réseau virtuelle configurée dans Proxmox VE.

Configuration des adresses IP.

Les adresses IP suivantes ont été attribuées :

— WAN : adresse IP obtenue automatiquement (DHCP)

— LAN : 192.168.1.1 /24

— DMZ : 192.168.2.1 /24

Cette configuration permet de segmenter le réseau et d'isoler les différents types de flux.

Objectif :

La configuration des interfaces permet d'organiser le réseau en différentes zones afin d'améliorer la sécurité et de faciliter la gestion des communications.

4.2 Configuration LAN

L'interface LAN a été configurée sur le pare-feu pfSense afin de représenter le réseau interne de l'entreprise.

Objectif.

Le réseau LAN (Local Area Network) permet de connecter les machines internes de l'infrastructure, notamment le serveur Windows (Active Directory) et les postes clients.

Il constitue le réseau principal sur lequel les utilisateurs travaillent et accèdent aux ressources de l'entreprise.

Configuration.

L'interface LAN a été associée à une carte réseau virtuelle connectée à un bridge interne sur Proxmox VE.

Les paramètres suivants ont été définis :

Adresse IP du LAN : 192.168.1.1 Masque de sous-réseau : 255.255.255.0 (/24) Activation du serveur DHCP pour distribuer automatiquement les adresses IP aux machines clientes.

Le pare-feu attribue ainsi automatiquement une adresse IP aux postes connectés au réseau LAN.

Rôle dans l'infrastructure.

L'interface LAN permet :

La communication entre les machines internes. L'accès aux services du serveur (Active Directory, DNS). L'accès à Internet via le pare-feu. La gestion centralisée des utilisateurs et des postes.

Sécurité.

Par défaut, le pare-feu autorise les communications sortantes depuis le LAN vers les autres réseaux, tout en permettant de contrôler les flux grâce à des règles de filtrage.

Cette configuration garantit un bon équilibre entre accessibilité et sécurité.

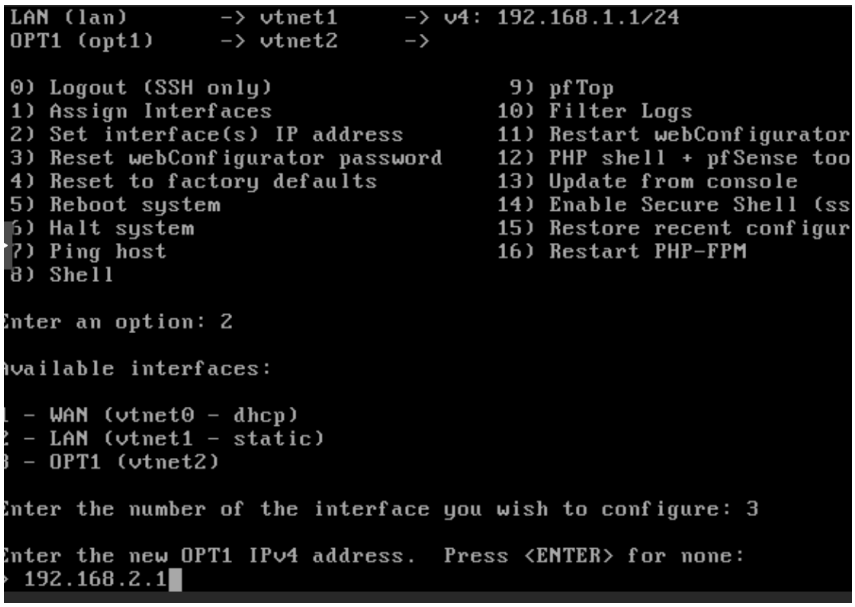

Figure 4.1 – LAN

Chapitre 5

Installation de Windows Server

5.1 Installation du système

Dans le cadre de la mise en place de l'infrastructure, un serveur Windows a été déployé sous forme de machine virtuelle afin d'assurer le rôle de contrôleur de domaine.

Cette machine a été installée sur l'hyperviseur Proxmox VE.

Étapes d'installation.

— Création d'une machine virtuelle dédiée
— Attribution des ressources matérielles (CPU, RAM, stockage)
— Montage de l'image ISO de Windows Server
— Démarrage de la machine et lancement de l'installation

L'installation du système a été réalisée en suivant les étapes classiques de Windows Server, incluant :

— le choix de la langue et du clavier ;
— la sélection de la version du système ;
— la configuration du disque.

Une fois l'installation terminée, le serveur a été configuré avec un mot de passe administrateur sécurisé.

Objectif :

Cette étape permet de mettre en place un serveur capable d'héberger les services nécessaires à la gestion centralisée de l'infrastructure, notamment Active Directory.

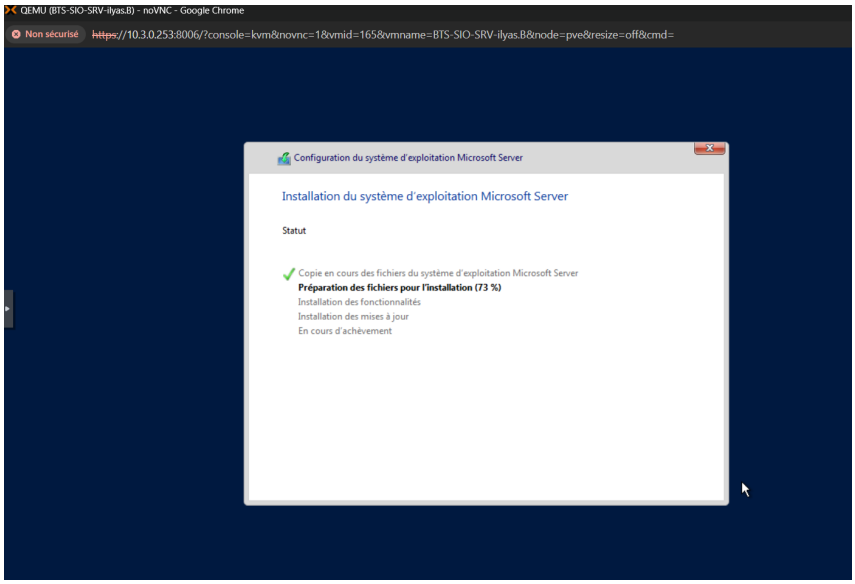

FIGURE 5.1 – SRV

5.2 Configuration réseau

Configuration réseau.

Après l'installation du système, la configuration réseau du serveur a été réalisée afin de l'intégrer correctement au réseau LAN.

Configuration.

Une adresse IP statique a été attribuée au serveur afin de garantir sa disponibilité sur le réseau.

Les paramètres suivants ont été définis :

Adresse IP : 192.168.1.10 Masque de sous-réseau : 255.255.255.0 Passerelle par défaut : 192.168.1.1 Serveur DNS : 192.168.1.10

L'utilisation d'une adresse IP fixe est essentielle pour un serveur, notamment pour assurer le bon fonctionnement des services réseau comme Active Directory et DNS.

Objectif :

Cette configuration permet au serveur d'être accessible de manière fiable par les autres machines du réseau et de fournir des services critiques de manière stable.

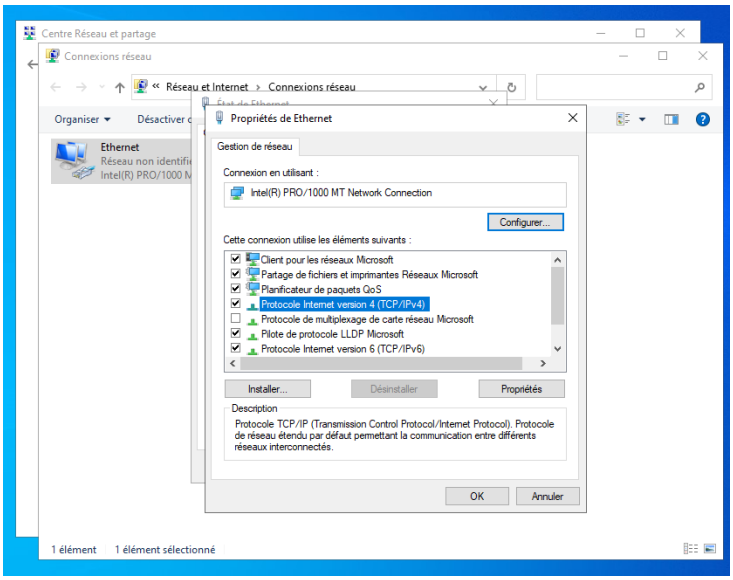

FIGURE 5.2 –

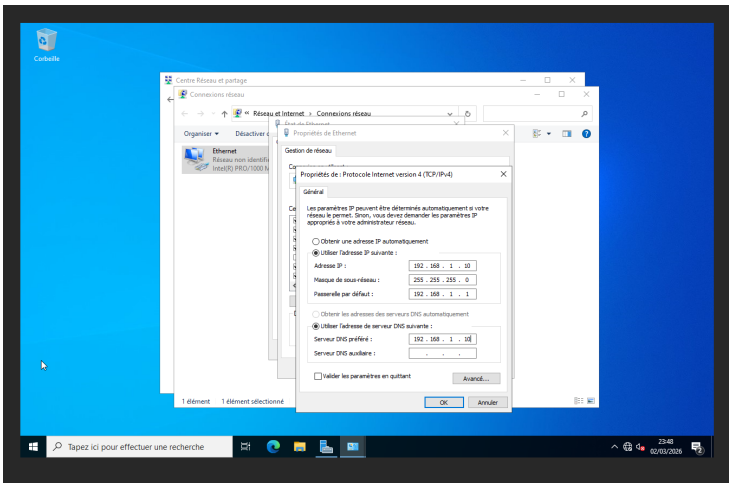

FIGURE 5.3 –

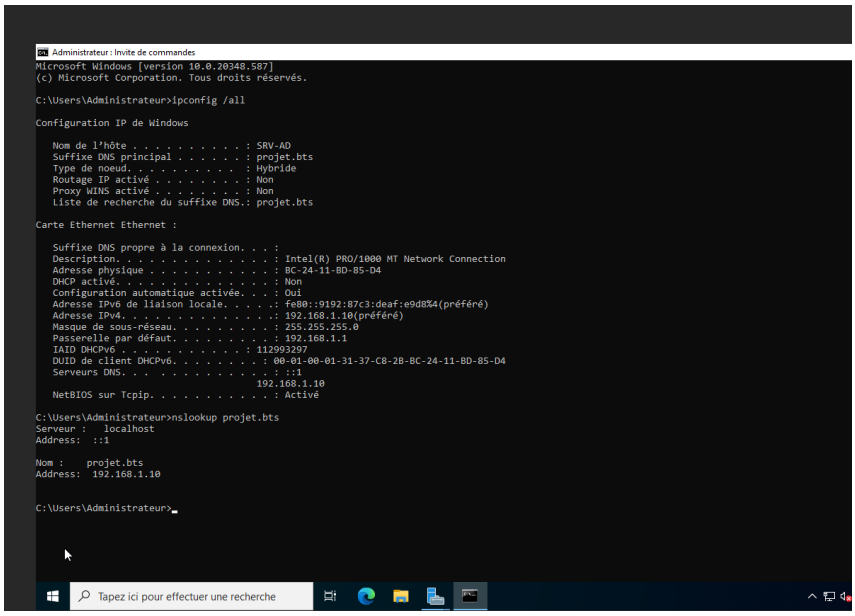

FIGURE 5.4 –

5.3 Tests de connectivité

Après la configuration réseau, des tests de connectivité ont été réalisés afin de vérifier le bon fonctionnement du réseau.

Tests effectués.

— Test de communication avec le pare-feu : ping 192.168.1.1

— Test d'accès à Internet : ping 8.8.8.8

— Vérification de la configuration IP : ipconfig

Résultats.

Les tests ont permis de valider :

— la communication entre le serveur et le pare-feu ;

— l'accès au réseau externe ;

— la bonne configuration de l'adressage IP.

Objectif.

Ces vérifications sont essentielles pour s'assurer que le serveur est correctement intégré au réseau avant la mise en place des services tels qu'Active Directory.

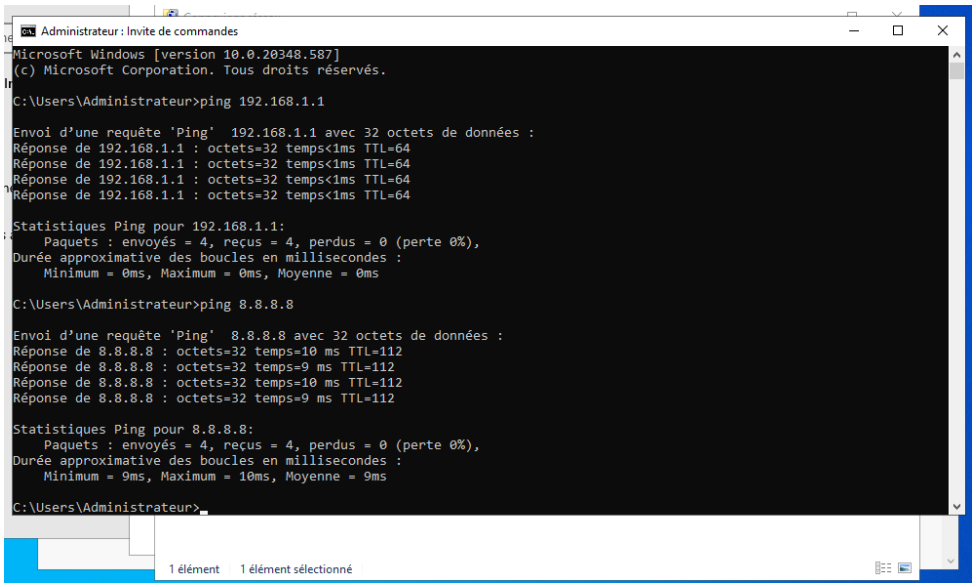

FIGURE 5.5 – Test

Chapitre 6

Mise en place de l'Active Directory

6.1 Installation des rôles

Afin de mettre en place un annuaire centralisé, le rôle Active Directory Domain Services (AD DS) a été installé sur le serveur Windows.

Cette installation a été réalisée via le gestionnaire de serveur en ajoutant le rôle AD DS ainsi que les fonctionnalités associées.

L'installation de ce rôle permet de transformer le serveur en contrôleur de domaine et de gérer les utilisateurs, les groupes et les ressources du réseau.

6.2 Création du domaine projet.bts

Après l'installation du rôle AD DS, le serveur a été promu en contrôleur de domaine.

Un nouveau domaine a été créé avec le nom suivant :

projet.bts

Ce domaine permet de centraliser l'authentification et la gestion des machines et utilisateurs du réseau.

6.3 Configuration DNS

Le service DNS a été automatiquement installé avec Active Directory.

Il permet la résolution des noms de domaine en adresses IP.

Le serveur DNS a été configuré pour pointer vers lui-même, garantissant le bon fonctionnement des services du domaine.

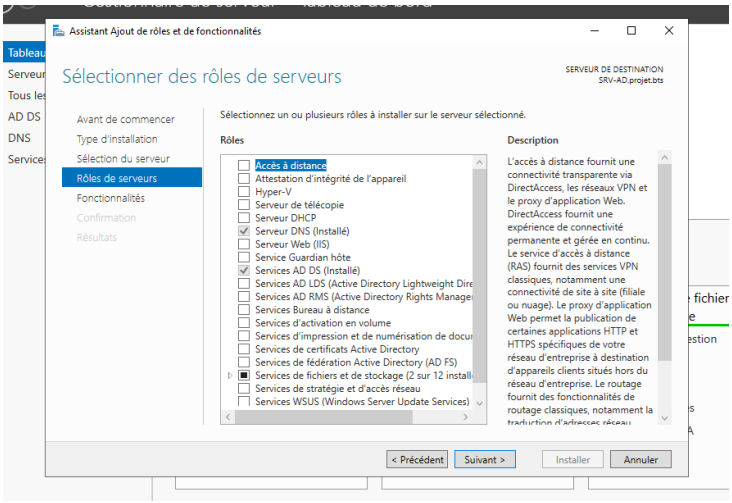

FIGURE 6.1 –

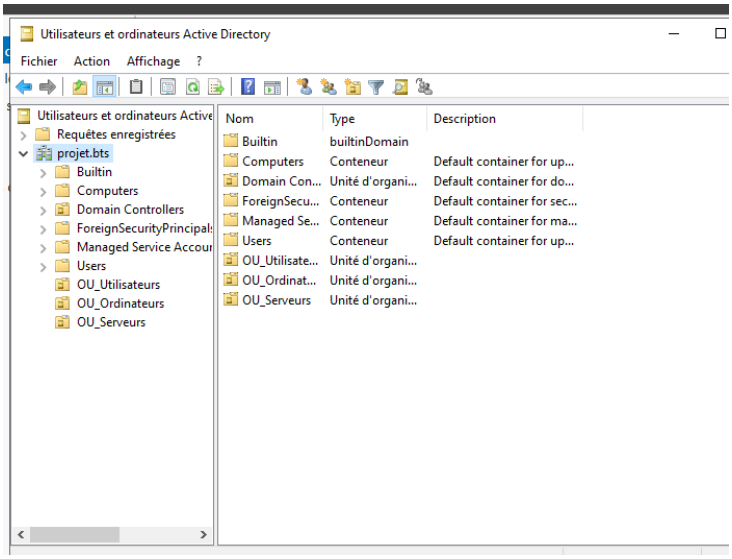

FIGURE 6.2 –

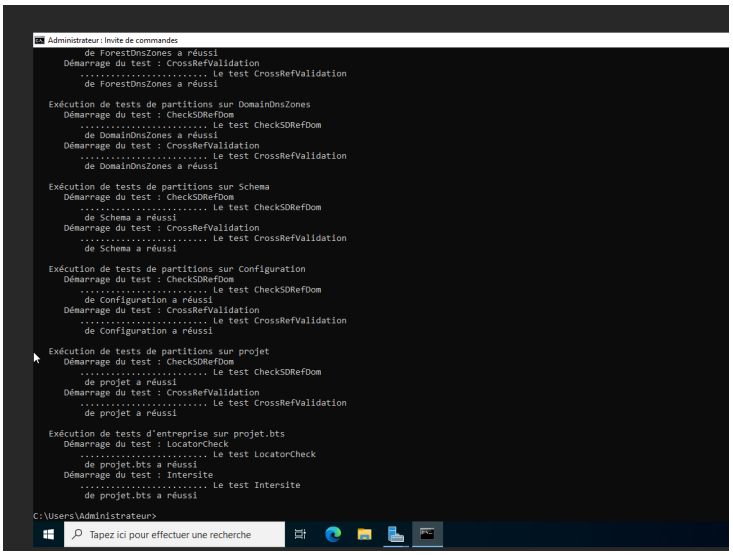

FIGURE 6.3 –

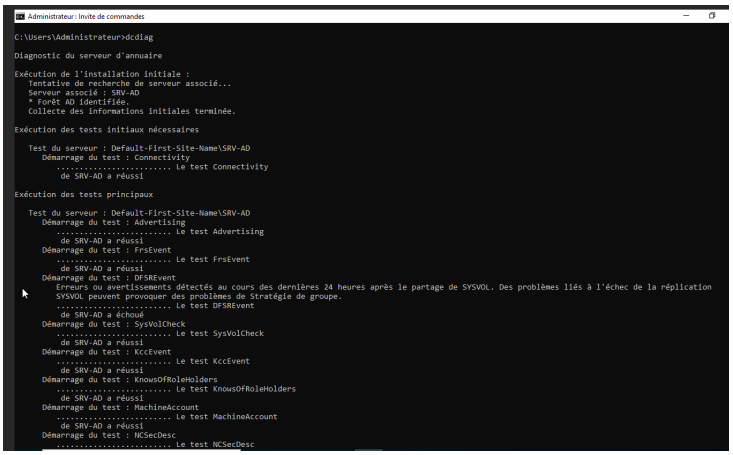

FIGURE 6.4 –

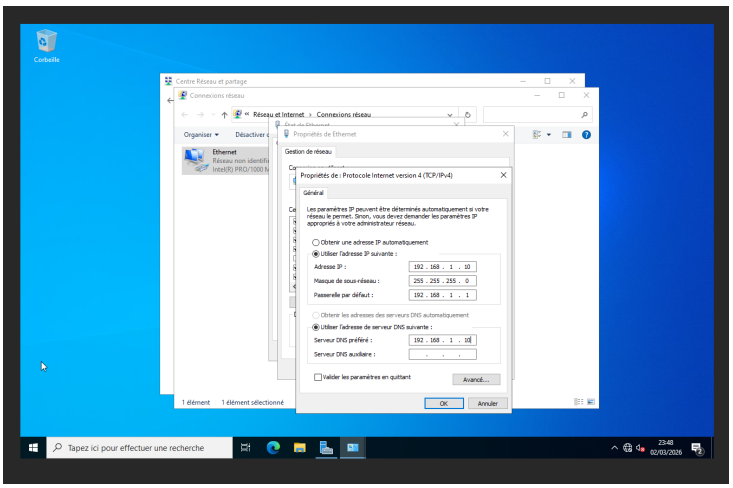

FIGURE 6.5 –

Chapitre 7

Organisation de l'Active Directory

7.1 Création des OU

Des unités d'organisation (OU) ont été créées afin de structurer l'annuaire Active Directory.

Les OU suivantes ont été mises en place :

— Comptabilité
— RH
— Informatique

Cette organisation permet de gérer les utilisateurs et les machines de manière structurée.

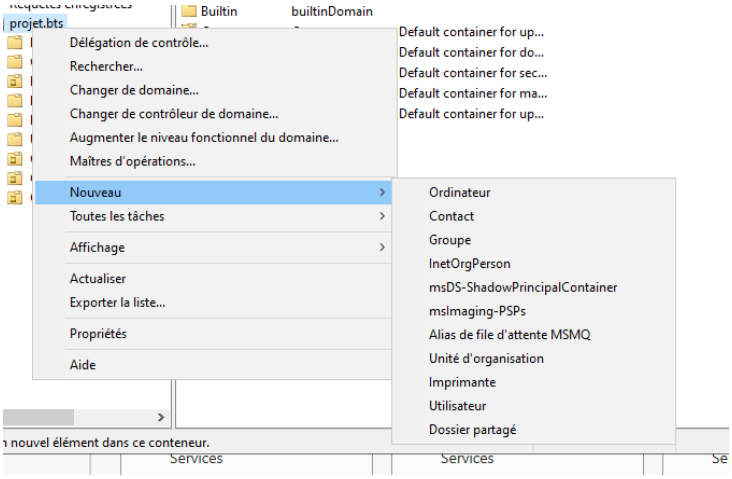

FIGURE 7.1 –

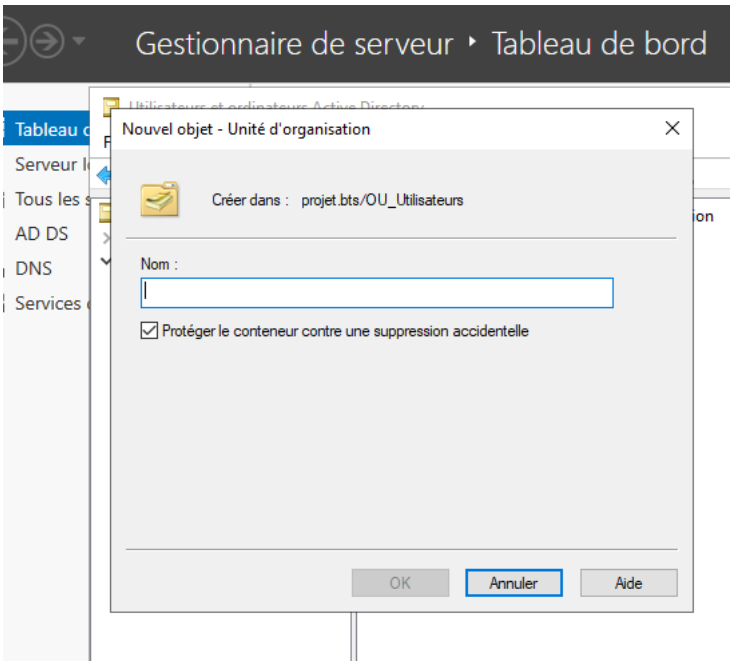

FIGURE 7.2 –

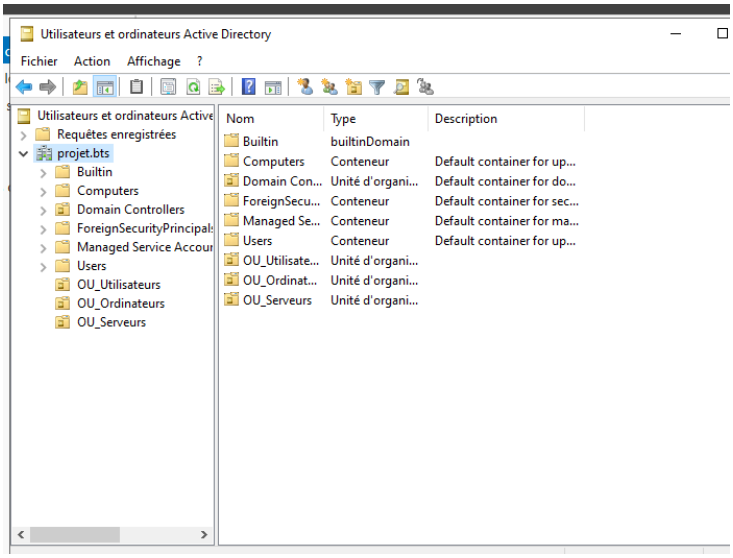

FIGURE 7.3 –

7.2 Création des utilisateurs

Des groupes de sécurité ont été créés afin de gérer les droits d'accès.

Ces groupes permettent d'attribuer des permissions de manière globale à plusieurs utilisateurs. Des comptes utilisateurs ont été créés pour chaque service de l'entreprise.

Chaque utilisateur est associé à une OU spécifique, ce qui facilite la gestion et l'application des stratégies.

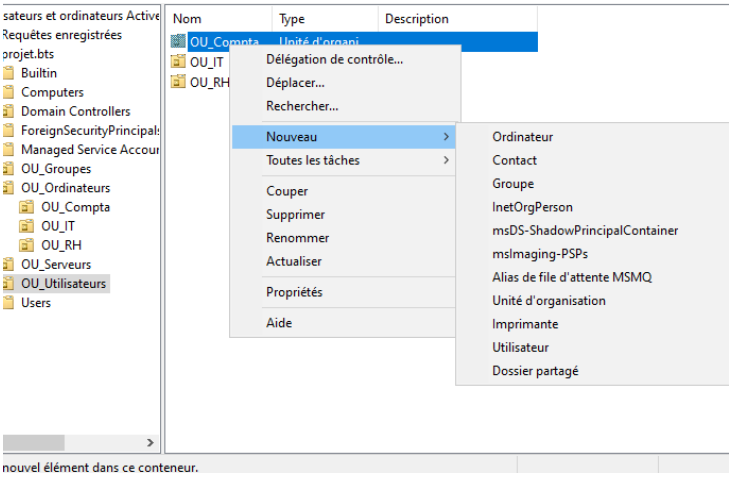

FIGURE 7.4 – Enter Caption

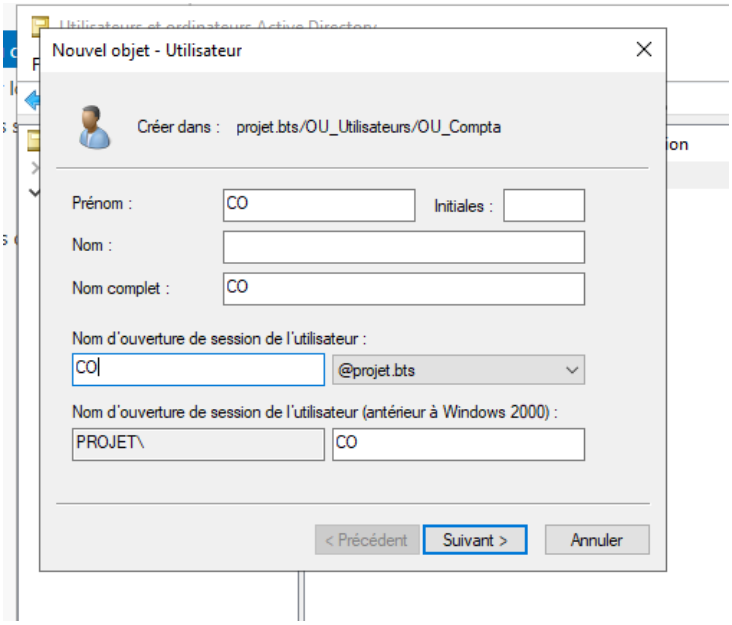

FIGURE 7.5 –

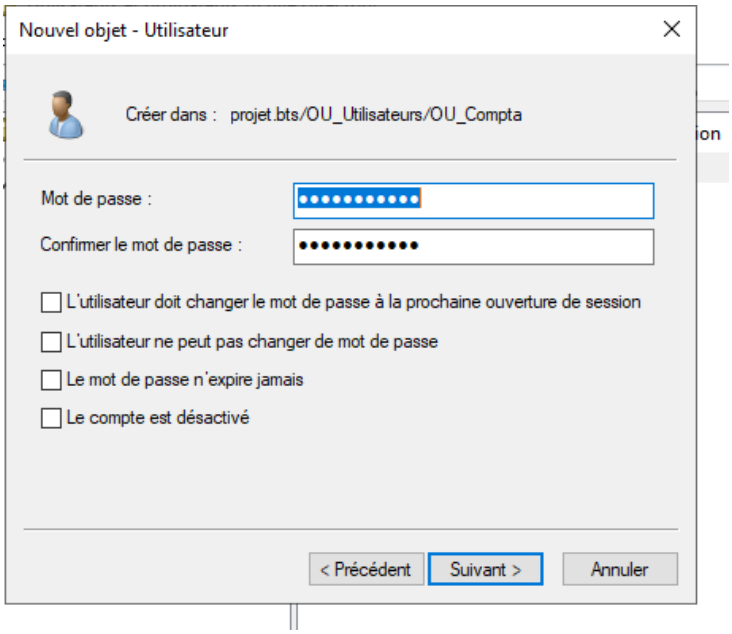

FIGURE 7.6 –

7.3 Création des groupes

Des groupes de sécurité ont été créés afin de gérer les droits d'accès.

Ces groupes permettent d'attribuer des permissions de manière globale à plusieurs utilisateurs.

7.4 Organisation des ressources

Les ressources (utilisateurs, groupes, ordinateurs) ont été organisées dans les différentes OU afin de simplifier l'administration et la gestion des droits.

Chapitre 8

Installation des postes clients

8.1 Création des machines

Plusieurs machines clientes ont été créées afin de simuler les postes de travail de l'entreprise (Comptabilité, RH, Informatique).

Ces machines ont été déployées sous forme de machines virtuelles.

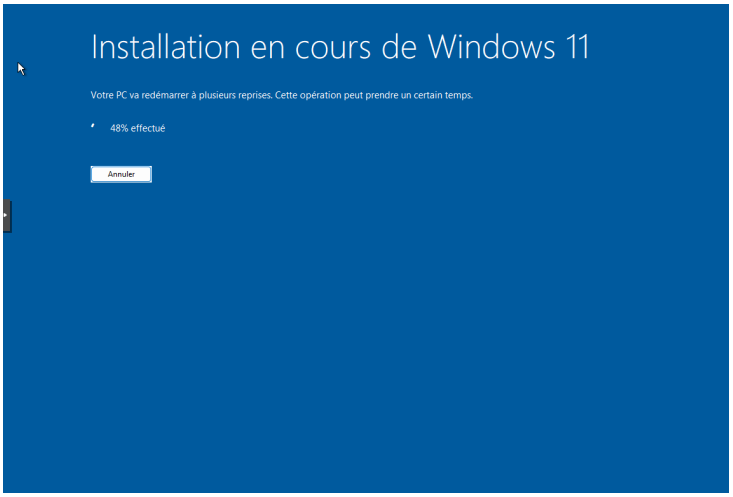

FIGURE 8.1 –

8.2 Configuration réseau (DHCP)

Les postes clients ont été configurés pour obtenir automatiquement une adresse IP via le serveur DHCP configuré sur le pare-feu pfSense.

Cette configuration permet une gestion automatique et simplifiée des adresses IP.

8.3 Tests réseau

Des tests ont été réalisés afin de vérifier la connectivité :

— ping vers la passerelle
— ping vers le serveur
— vérification de l'adresse IP avec ipconfig

Ces tests permettent de valider le bon fonctionnement du réseau.

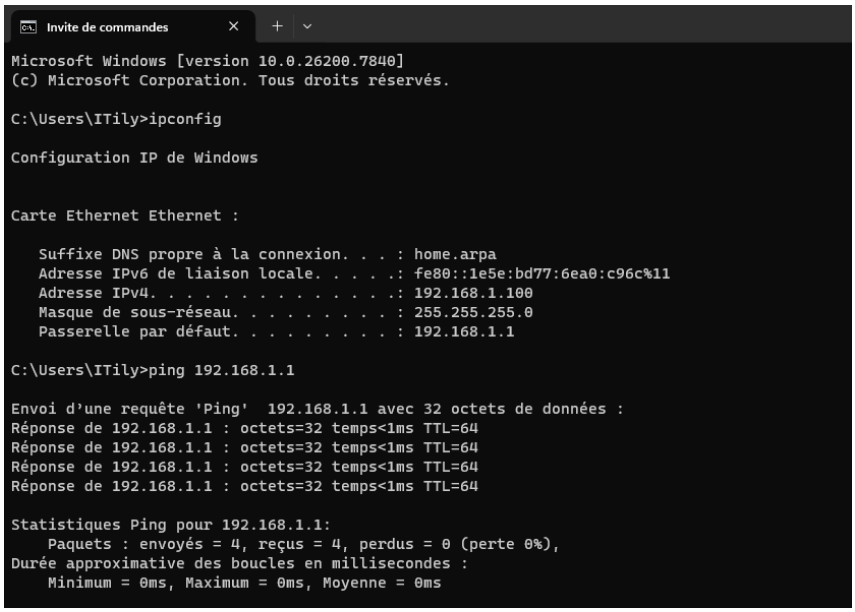

FIGURE 8.2 –

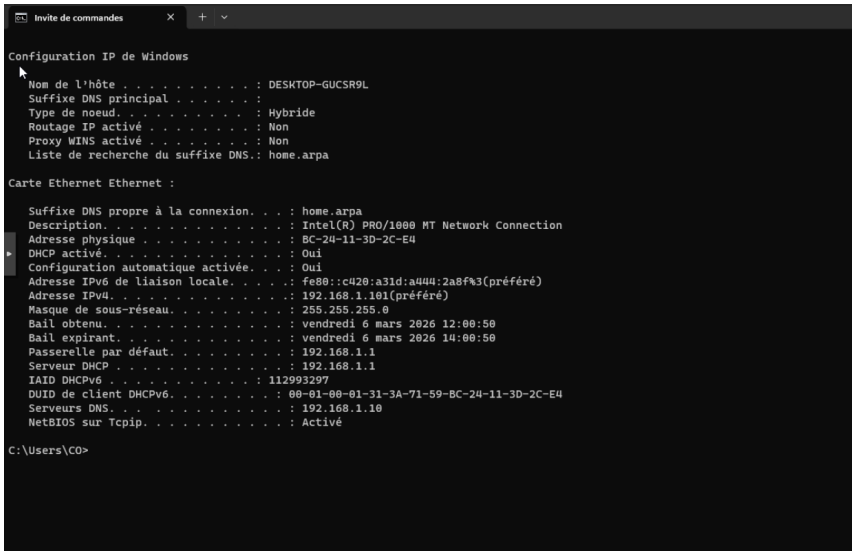

FIGURE 8.3 –

Chapitre 9

Intégration au domaine

9.1 Jonction au domaine projet.bts

Les machines clientes ont été intégrées au domaine **projet.bts**.
Cette opération permet aux utilisateurs de se connecter avec un compte centralisé.

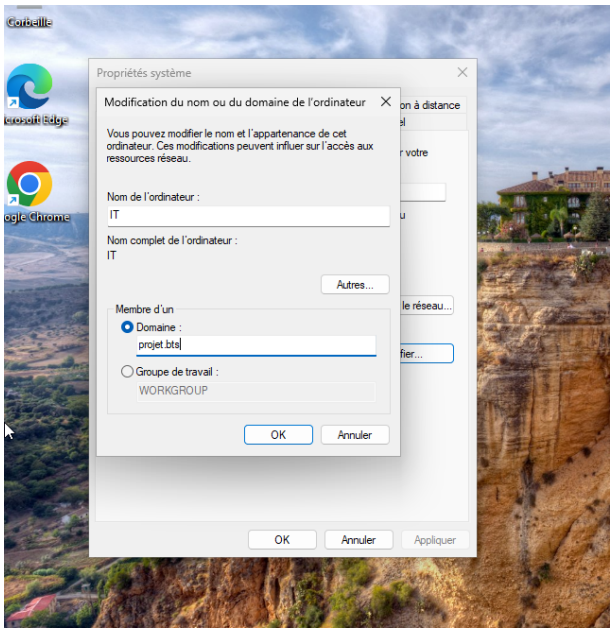

FIGURE 9.1 –

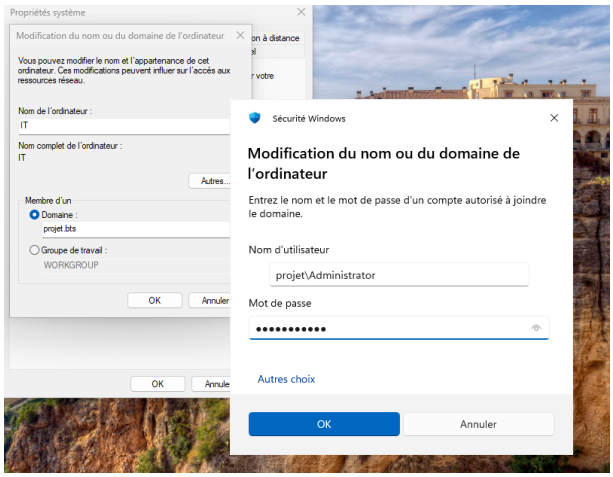

FIGURE 9.2 –

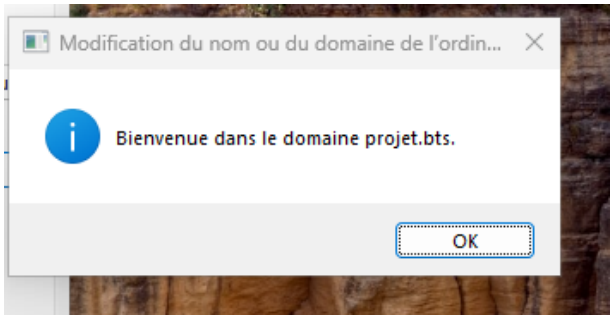

FIGURE 9.3 –

9.2 Validation de la connexion

Après l'intégration, des tests ont été réalisés :
— Connexion avec un compte du domaine
— Vérification de l'accès aux ressources
Ces tests confirment la bonne intégration au domaine.

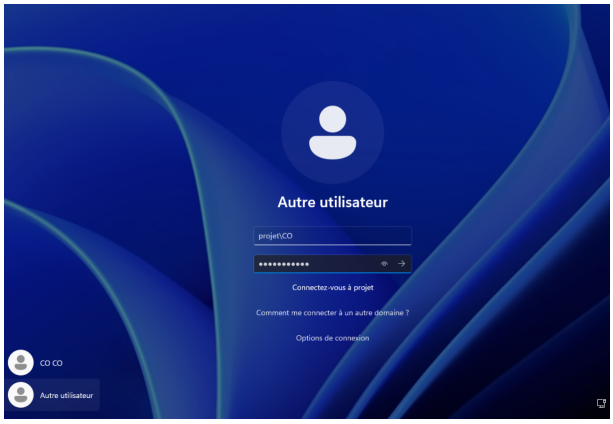

FIGURE 9.4 –

Chapitre 10

Gestion des droits

Un compte utilisateur nommé **it.tech** a été créé afin de disposer d'un compte avec des droits élevés pour l'administration.

10.1 Création du compte it.tech

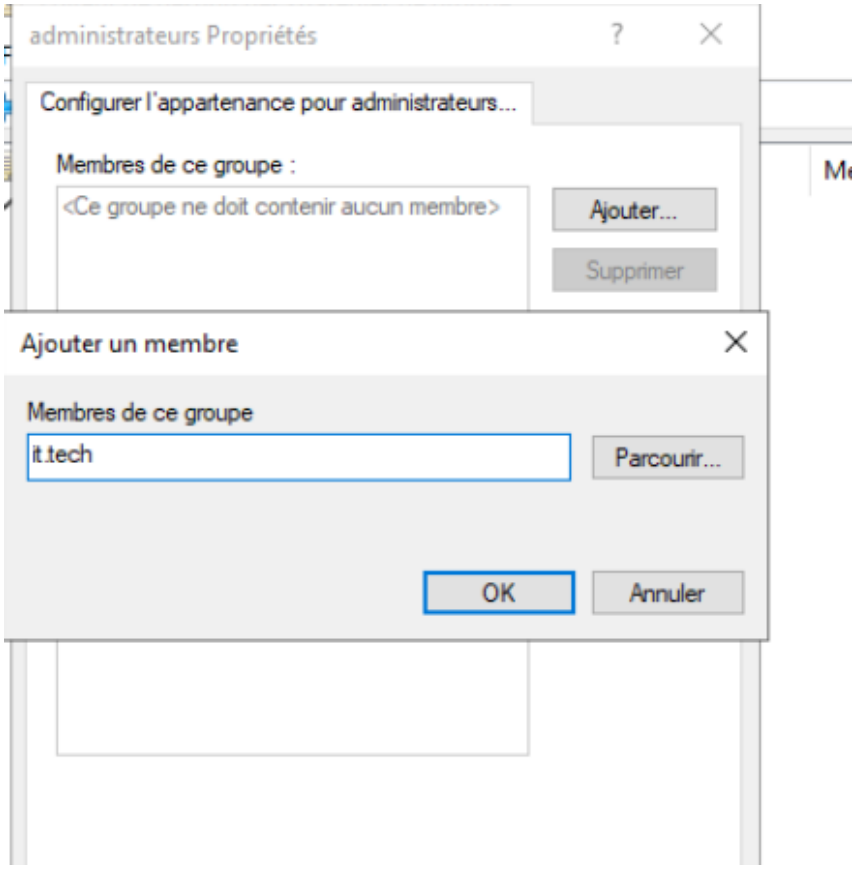

FIGURE 10.1 –

10.2 Gestion des permissions

Les permissions ont été configurées à l'aide de groupes afin de contrôler l'accès aux ressources.

Cette méthode permet une gestion plus simple et plus sécurisée des droits.

Chapitre 11

Configuration du pare-feu pfSense

11.1 Présentation des règles

Le pare-feu pfSense permet de contrôler les flux réseau à l'aide de règles de filtrage.

Chaque règle définit :

— une source

— une destination

— un protocole

— une action (autoriser ou bloquer)

Les règles sont appliquées de haut en bas, la première règle correspondante est appliquée.

Par défaut, pfSense bloque les connexions entrantes et autorise certaines communications sortantes selon la configuration.

11.2 Règles LAN vers WAN

Une règle a été mise en place afin d'autoriser les machines du réseau LAN à accéder à Internet.

Cette règle permet :

aux postes clients de naviguer sur Internet, au serveur d'accéder à des ressources externes, de tester la connectivité réseau.

Configuration de la règle :

— Source : LAN net

— Destination : any

— Protocole : any

— Action : Pass

Cette règle est essentielle pour permettre le fonctionnement normal du réseau interne.

11.3 Règles de blocage

Des règles de blocage ont été mises en place afin de renforcer la sécurité du réseau.

Ces règles permettent de :

— empêcher les accès non autorisés

— limiter les communications entre certaines zones

— protéger les machines internes

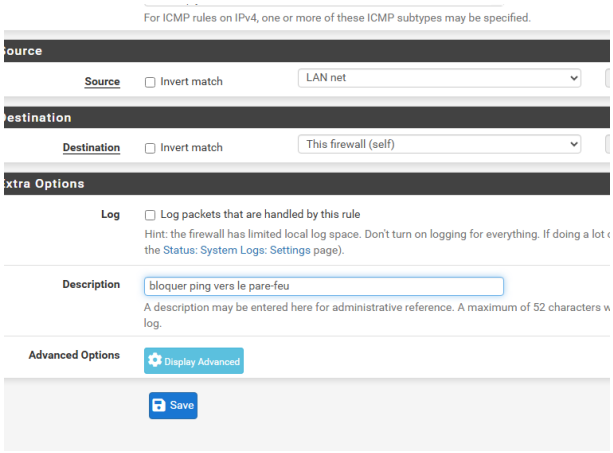

FIGURE 11.1 –

11.4 Règles spécifiques

Des règles spécifiques ont été configurées pour répondre à des besoins précis du projet. Par exemple :

— Autoriser la communication entre le serveur de supervision et les machines (port 10050 pour Zabbix)

— Autoriser certains flux nécessaires au fonctionnement des services (DNS, DHCP, etc.)

Ces règles permettent d'adapter le pare-feu aux besoins de l'infrastructure tout en maintenant un niveau de sécurité élevé.

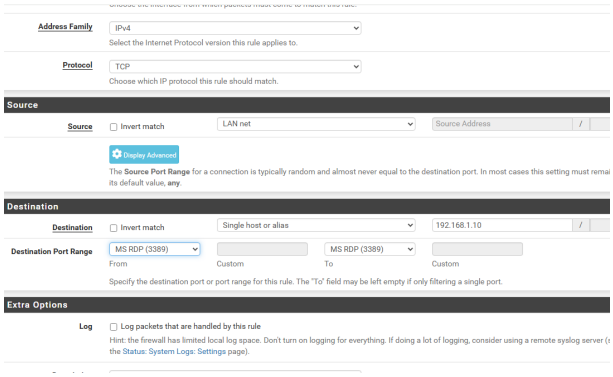

FIGURE 11.2 –

Chapitre 12

Mise en place de la DMZ

12.1 Ajout de l'interface DMZ

Une troisième interface réseau a été ajoutée sur le pare-feu pfSense afin de créer une zone DMZ.

Cette interface a été reliée à un réseau virtuel dédié sur Proxmox VE.

L'ajout de cette interface permet de séparer physiquement et logiquement les réseaux internes et externes.

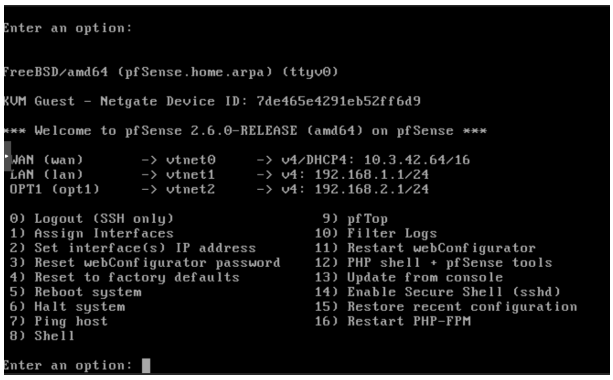

FIGURE 12.1 –

12.2 Configuration du réseau DMZ

L'interface DMZ a été configurée avec les paramètres suivants :

— Adresse IP : 192.168.2.1

— Masque de sous-réseau : 255.255.255.0

Les machines présentes dans cette zone utilisent cette interface comme passerelle.

Cette configuration permet de créer un réseau isolé du LAN.

12.3 Objectif de la DMZ

La DMZ (zone démilitarisée) permet d'héberger des services accessibles depuis l'extérieur tout en protégeant le réseau interne.

Elle offre :

— Une isolation des services exposés

— Une réduction des risques en cas d'attaque
— Un contrôle des flux réseau
Cette architecture renforce la sécurité globale de l'infrastructure.

Chapitre 13

Installation du serveur Linux

13.1 Installation du système

Un serveur Linux a été déployé dans la DMZ afin d'héberger un service web.
Le système a été installé sous forme de machine virtuelle sur Proxmox VE.
L'installation a été réalisée en mode minimal afin d'optimiser les ressources.

13.2 Configuration IP

Une adresse IP statique a été attribuée au serveur :
— Adresse IP : 192.168.2.10
— Masque : 255.255.255.0
— Passerelle : 192.168.2.1
Cette configuration permet au serveur de communiquer avec le pare-feu et les autres réseaux.

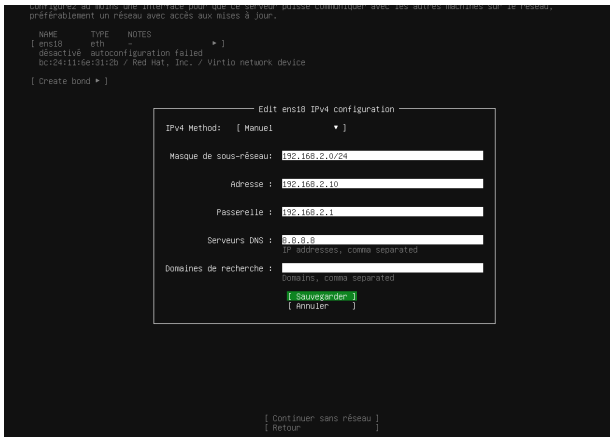

Figure 13.1 –

13.3 Tests réseau

Des tests ont été réalisés pour vérifier la connectivité :
— ping vers la passerelle (192.168.2.1)
— ping vers le LAN

— ping vers Internet
Ces tests permettent de valider le bon fonctionnement du réseau.

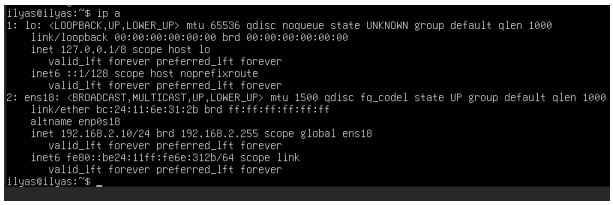

Figure 13.2 –

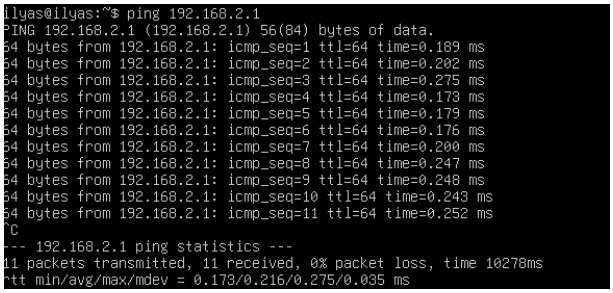

Figure 13.3 –

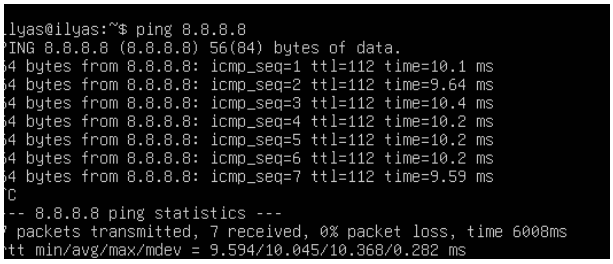

Figure 13.4 –

Chapitre 14

Installation du serveur web

14.1 Installation Apache

Un serveur web a été installé sur la machine Linux à l'aide du serveur Apache.
Commande utilisée :
— sudo apt install apache2 -y
Apache permet d'héberger des pages web accessibles via le réseau.

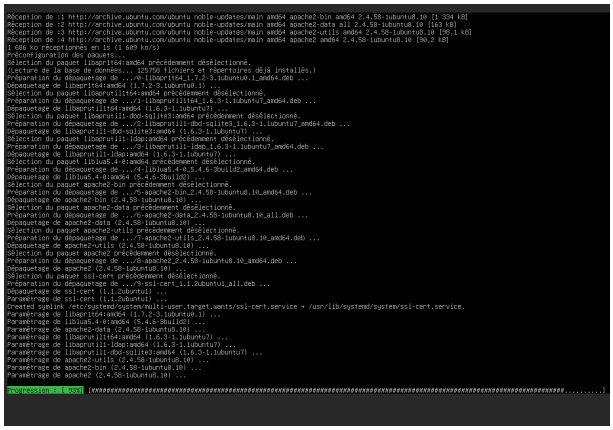

FIGURE 14.1 –

14.2 Vérification du service

Le bon fonctionnement du service a été vérifié avec la commande :
— sudo systemctl status apache2
Le service doit être actif (running).

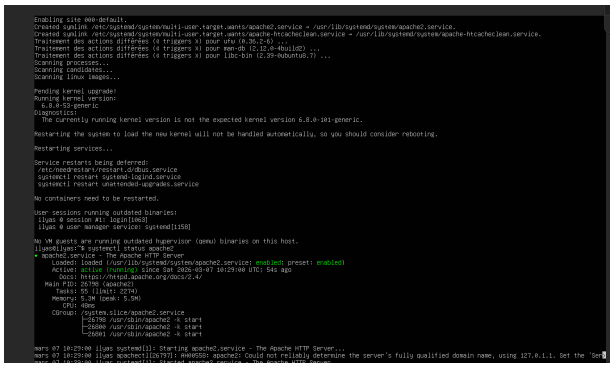

FIGURE 14.2 –

14.3 Accès au serveur web

L'accès au serveur web a été testé depuis une machine du réseau LAN via un navigateur.

Adresse utilisée :

— http ://192.168.2.10

L'affichage de la page par défaut Apache confirme le bon fonctionnement du serveur web.

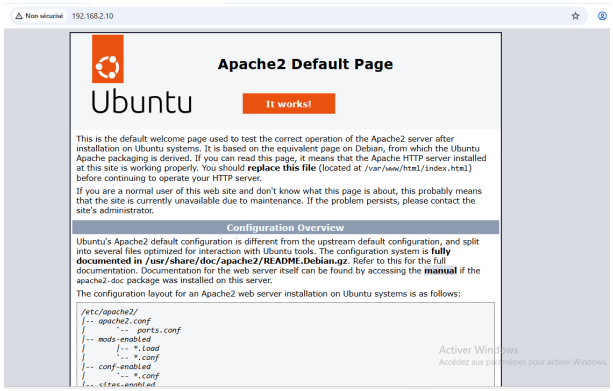

FIGURE 14.3 –

Chapitre 15

Tests et validation

15.1 Tests de connectivité

Des tests de connectivité ont été réalisés entre les différentes machines :
— ping entre LAN et DMZ
— ping vers le pare-feu
— accès à Internet
Ces tests permettent de vérifier la communication réseau.

15.2 Tests d'accès

Des tests ont été effectués pour vérifier l'accès aux services :
— accès au serveur web depuis le LAN
— connexion des utilisateurs au domaine
— accès aux ressources partagées

15.3 Problèmes rencontrés

Plusieurs problèmes ont été rencontrés :

1. Absence de communication réseau
2. Mauvaise configuration des règles du pare-feu
3. Problèmes d'adressage IP

15.4 Solutions apportées

Les solutions suivantes ont été mises en place :

1. Ajout et correction des règles sur pfSense
2. Vérification des configurations IP
3. Tests progressifs avec la commande ping

15.5 Validation finale

L'ensemble des tests a permis de valider :

— Le bon fonctionnement du réseau
— La communication entre les différentes zones
— L'accès aux services
Le projet est donc fonctionnel et conforme aux objectifs définis.