



CYCLE DE FORMATION
TECHNICIEN RÉSEAUX, SYSTEME ET SECURITÉ
INFORMATIQUE
Titre RNCP – Niveau 5

PROJET DE FIN D'ETUDES

SUJET :
Mise en place d'une solution d'accès
distant sécurisé avec RDP, Active
Directory et PfSense

RÉALISÉ par : Darius ILOKI

Période du 11 Février 2025 - 11 Mars 2025



Remerciements

Ce projet a été réalisé de manière autonome, mais il n'aurait pas été possible sans le soutien et les précieux conseils de ceux qui m'ont accompagné. Je tiens particulièrement à remercier **M. SIDIBE MAMOUTOU**, mon formateur support informatique, pour son accompagnement et son expertise, ainsi que **M. Lahoucine EL KAMEL**, mon responsable de stage, pour son encadrement et ses conseils précieux. Leur aide a été déterminante dans la réussite de ce projet.



Table des matières

1. INTRODUCTION	5
1.1 RESUME.....	5
1.2 ABSTRACT	5
1.3 PRESENTATION PERSONNELLE	5
2. PRESENTATION DU PROJET	5
2.1 CONTEXTE ET ENJEUX	5
2.2 OBJECTIFS ET PROBLEMATIQUE	6
3. EXPRESSION DES BESOINS	7
3.1 ANALYSE FONCTIONNELLE	7
3.2 CAHIER DES CHARGES	7
3.3 GESTION DES RISQUES ET DES ENJEUX	8
3.4 Topologie logique du projet	9
4. PLAN D'IMPLEMENTATION	10
5. REALISATION.....	11
5.1 Installation et configuration de Windows Server 2022	11
5.1.1 : Installation et configuration de l'Active Directory, windows 10 et 11, DNS et gestion via PowerShell	11
5.1.1.1 Installation du rôle Active Directory Domain Services (ADDS).....	12
5.1.1.2 Création du domaine Active Directory et promouvoir ce serveur en contrôleur de domaine.....	14
5.1.1.3 Configuration du serveur DNS	17
5.1.1.4 Gestion des utilisateurs, groupes et unités d'organisation via PowerShell.	21
5.1.1.4.1 Vérification des enregistrements SRV nécessaires pour le bon fonctionnement de l'Active Directory.	23
5.1.1.4.2 Mise en place des GPO pour le lecteur mappé.	24
5.1.1.4.3 Installation des Windows 10 et 11	25
5.1.2 CONFIGURATION DE PFSense	27
5.1.2.2 Configuration de l'authentification LDAP avec Active Directory.....	29
5.1.2.3 Génération des certificats auto-signés pour sécuriser OpenVPN	32
5.1.2.4 Installation et configuration d'OpenVPN pour l'accès distant sécurisé.....	34
6. TESTS ET VALIDATION	36
7. PERSPECTIVES D'ÉVOLUTION	41
8. CONCLUSION	42



Figure 1 : Installation de l'Active Directory.	11
Figure 2 : Ajout des rôles et fonctionnalités.	12
Figure 3 : Sélection du rôle ADDS.	13
Figure 4 : Création du domaine.	14
Figure 5 : Promotion en contrôleur de domaine.	15
Figure 6 : Nom de domaine défini.....	16
Figure 7 : Fin de la promotion et redémarrage.	17
Figure 8 : Accès au gestionnaire DNS.	18
Figure 9 : Configuration DNS.	18
Figure 10 : Configuration de la zone de recherche indirecte.....	19
Figure 11 : Configuration de la zone zone de recherche directe.	20
Figure 12 : Vérification des enregistrements SRV.	20
Figure 13 : Gestion AD via PowerShell	22
Figure 14 : Vérification SRV avec PowerShell.....	23
Figure 15 : Mise en place des GPO.....	24
Figure 16 : Configuration des interfaces pfSense.....	27
Figure 17 : Attribution des adresses IP.....	28
Figure 18 : Accès à l'interface web de pfSense.....	29
Figure 19 : Configuration LDAP	29
Figure 20 : Ajout du serveur LDAP.....	31
Figure 21 : Test de connexion LDAP.....	31
Figure 22 : Génération d'un certificat.	32
Figure 23 : Création d'une autorité de certification.	32
Figure 24 : Certificat serveur pour OpenVPN.	33
Figure 25 : Configuration OpenVPN.	34
Figure 26 : Règles de pare-feu OpenVPN.....	34
Figure 27 : Règles de pare-feu LAN.....	35
Figure 28 : Règles de pare-feu WAN.	36
Figure 29 : Téléchargement du client OpenVPN.....	36
Figure 30 : Installation du client OpenVPN	37
Figure 31 : Connexion réussie au VPN.	38
Figure 32 : Attribution IP via OpenVPN.....	39
Figure 33 : Test de connectivité.....	39
Figure 34 : Accès aux ressources internes.	40
Figure 35 : Résumé de l'infrastructure	41



1. INTRODUCTION

1.1 RESUME

Dans un environnement où la sécurité informatique et la gestion centralisée des infrastructures réseau sont essentielles, ce projet propose la mise en place d'une **infrastructure sécurisée** reposant sur **Windows Server 2022** et **PfSense**.

L'objectif principal est d'assurer :

- ❖ **La gestion centralisée des utilisateurs** et des ressources via **Active Directory (AD)**.
- ❖ **La sécurisation du réseau** avec **PfSense**, utilisé comme pare-feu et serveur VPN.
- ❖ **L'application de stratégies de sécurité** grâce aux **GPO (Group Policy Objects)**.
- ❖ **L'accès distant sécurisé** via **OpenVPN**, permettant aux utilisateurs de se connecter en toute sécurité aux ressources internes de l'entreprise.

Ce projet met en œuvre une infrastructure robuste permettant d'améliorer l'administration des systèmes et la cybersécurité d'un réseau d'entreprise. Il intègre des solutions open-source et propriétaires afin de garantir **performance, évolutivité et protection des données**.

1.2 ABSTRACT

This project aims to set up an IT infrastructure based on Windows Server 2022 and PfSense. The main goal is to ensure centralized user management, implement security policies, and provide secure remote access via OpenVPN.

1.3 PRESENTATION PERSONNELLE

Après une formation en administration des systèmes et réseaux, j'ai acquis des compétences dans la gestion des infrastructures informatiques. Ce projet me permet de mettre en pratique mes connaissances en administration système, cybersécurité et gestion des accès distants.

2. PRESENTATION DU PROJET

2.1 CONTEXTE ET ENJEUX

Dans un contexte où la cybersécurité et la gestion efficace des infrastructures réseau sont devenues des priorités pour les entreprises, il est essentiel de mettre en place des solutions fiables et robustes. La multiplication des cyberattaques, l'essor du télétravail et la nécessité d'un contrôle strict des accès internes et externes imposent la mise en œuvre d'une infrastructure sécurisée et centralisée.



Ce projet vise à concevoir et déployer une infrastructure sécurisée en utilisant :

- ❖ **Windows Server 2022** pour la gestion des utilisateurs et des ressources réseau via **Active Directory**
- ❖ **PfSense** en tant que pare-feu et serveur VPN. L'objectif est d'offrir un environnement sécurisé, évolutif et efficace permettant d'assurer une connectivité fiable pour les employés et une gestion centralisée des accès.

2.2 OBJECTIFS ET PROBLEMATIQUE

2.2.1 OBJECTIFS

L'objectif de ce projet est d'assurer une gestion sécurisée des utilisateurs et des accès distants en mettant en place une infrastructure réseau basée sur **Windows Server 2022** et **PfSense**. Les objectifs spécifiques sont les suivants :

1. **Déploiement d'un domaine Active Directory (AD)** sur **Windows Server 2022** afin de centraliser la gestion des utilisateurs et des groupes.
2. **Configuration du DNS** pour assurer la résolution des noms de domaine internes et faciliter la communication entre les différentes machines du réseau.
3. **Création et gestion des unités organisationnelles (OU)**, des utilisateurs et des groupes via **PowerShell**, afin d'automatiser et de sécuriser l'administration du domaine.
4. **Mise en place de stratégies de groupe (GPO)** pour appliquer des configurations automatisées et standardisées, comme l'attribution automatique de lecteurs réseau.
5. **Installation et configuration de PfSense** en tant que pare-feu et serveur VPN pour sécuriser les accès au réseau.
6. **Intégration de PfSense avec Active Directory via LDAP**, permettant une authentification centralisée et un contrôle des accès basé sur les groupes AD.
7. **Génération et mise en place de certificats auto-signés** pour assurer un chiffrement des communications VPN.
8. **Configuration et test d'OpenVPN** pour permettre un accès distant sécurisé aux ressources internes du réseau.

Ces étapes permettront de garantir une infrastructure sécurisée, performante et facile à administrer.



2.2.2 PROBLEMATIQUE

Dans un contexte où les cyberattaques sont de plus en plus fréquentes et où la gestion des accès distants devient un enjeu crucial, la question centrale de ce projet est la suivante :

Comment garantir une gestion efficace et sécurisée des utilisateurs et des accès distants en intégrant Windows Server 2022 et PfSense ?

Cette problématique met en évidence les défis liés à l'administration des infrastructures informatiques modernes, notamment en matière de sécurisation des accès, centralisation de la gestion des utilisateurs et évolutivité du système.

3. EXPRESSION DES BESOINS

3.1 ANALYSE FONCTIONNELLE

Le projet répond aux besoins suivants :

- ❖ Authentification centralisée des utilisateurs
- ❖ Automatisation des tâches administratives
- ❖ Contrôle des accès et filtrage du trafic
- ❖ Accès distant sécurisé via VPN

3.2 CAHIER DES CHARGES

Élément	Détails
OpenVPN	Accès distant sécurisé
Windows Server 2022	Gestion des utilisateurs (AD), DNS, GPO
PfSense	Pare-feu, gestion du réseau, serveur VPN
machine Windows 10	Membre du Domain AD, Bureau à distance
Client Windows 10	Test de connexion VPN et application des stratégies
PowerShell	Automatisation des tâches administratives
VMware Workstation Pro	Virtualisation des serveurs et clients

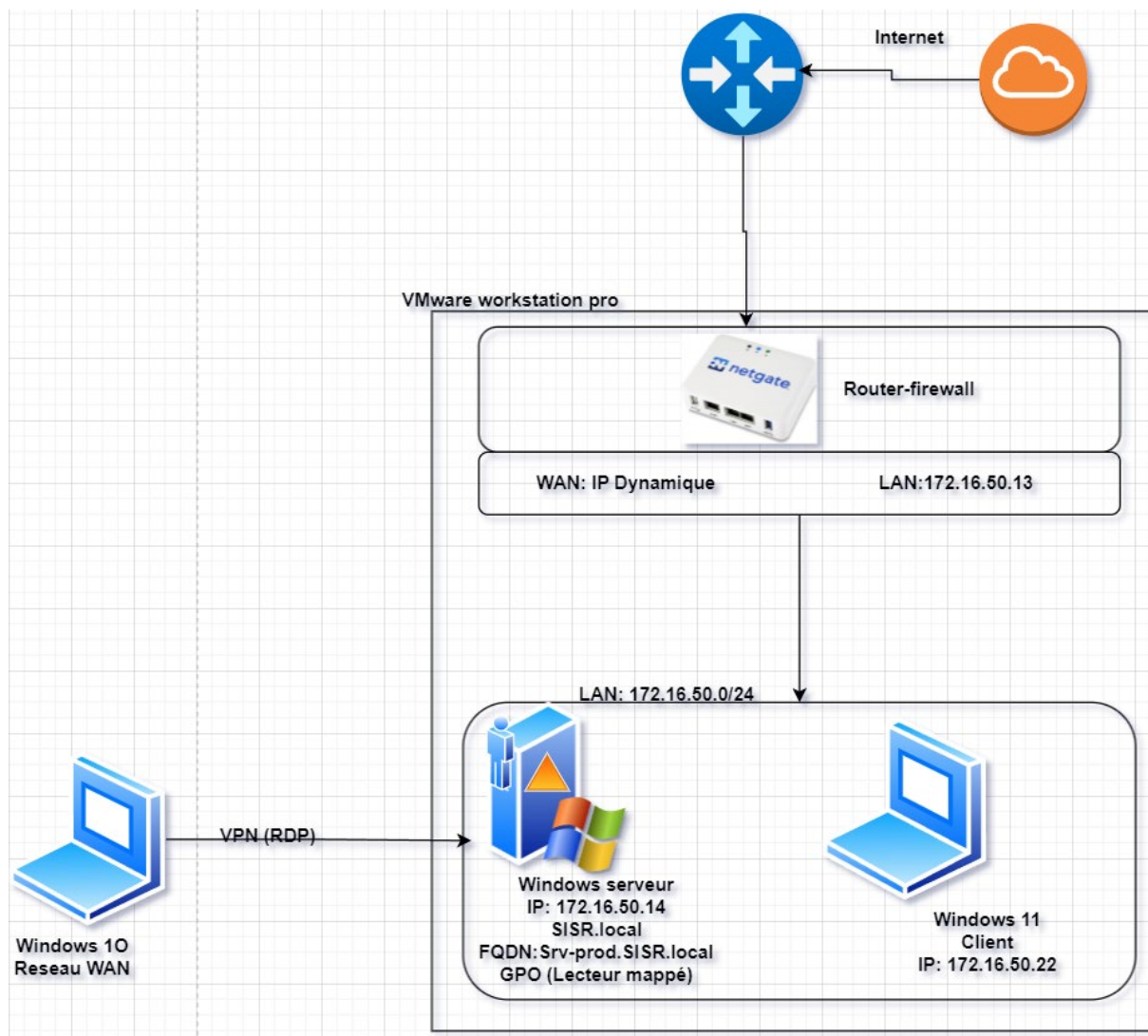


3.3 GESTION DES RISQUES ET DES ENJEUX

ID	Risque/Enjeu	Impact	Probabilité	Criticité
R1	Échec de l'authentification LDAP	Accès bloqué	Moyenne	Élevée
R2	Mauvaise configuration des GPO	Perte d'efficacité	Haute	Moyenne
E1	Sécurisation du VPN	Connexion chiffrée	-	-
E2	Évolutivité du système	Intégration future	-	-



3.4 Topologie logique du projet





4. PLAN D'IMPLEMENTATION

1. Installation et configuration de Windows Server 2022 avec AD et DNS.
2. Création et gestion des utilisateurs et groupes via PowerShell.
3. Mise en place des GPO pour automatiser l'environnement utilisateur.
4. Installation et configuration de PfSense avec les interfaces WAN et LAN.
5. Intégration de PfSense au domaine via LDAP.
6. Génération de certificats auto-signés pour sécuriser OpenVPN.
7. Mise en place d'OpenVPN et exportation des profils.
8. Tests et validation de la connexion VPN et de l'application des GP



5. REALISATION

5.1 Installation et configuration de Windows Server 2022

5.1.1 : Installation et configuration de l'Active Directory, windows 10 et 11, DNS et gestion via PowerShell

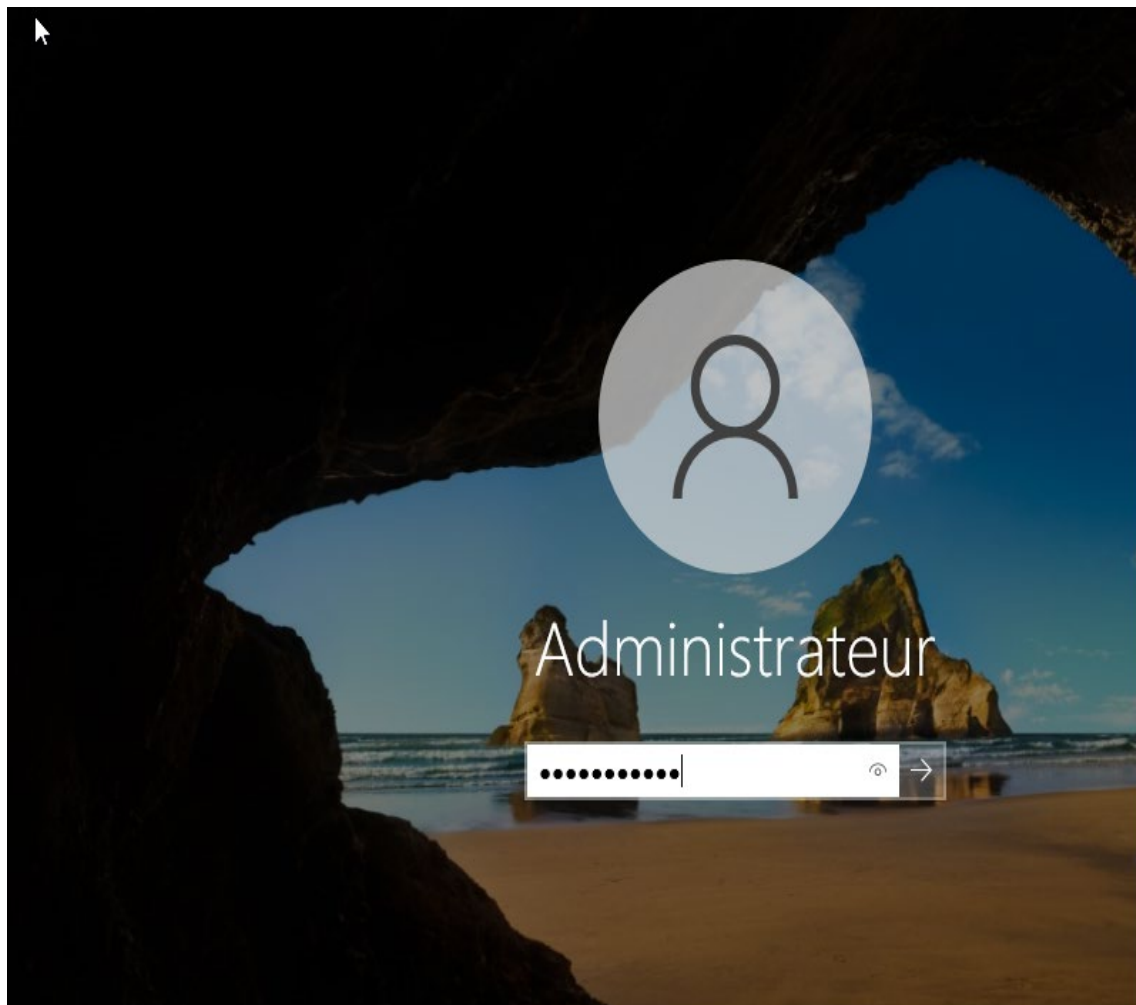


Figure 1



Dans ce projet, l'installation de l'infrastructure Active Directory (AD) a été réalisée de manière autonome. Le processus a suivi les étapes suivantes :

- ❖ **Installation du rôle Active Directory Domain Services (ADDS)**
- ❖ **Création du domaine Active Directory**
- ❖ **Configuration du serveur DNS pour l'Active Directory**
- ❖ **Gestion des utilisateurs, groupes et unités d'organisation (OU) via PowerShell**

5.1.1.1 Installation du rôle Active Directory Domain Services (ADDS)

La première étape a été l'installation du rôle **Active Directory Domain Services (ADDS)**. Ce rôle est essentiel pour permettre à un serveur d'agir en tant que **contrôleur de domaine** dans l'infrastructure de l'entreprise.

Étapes suivies :

1. **Ouverture du Gestionnaire de serveur.**

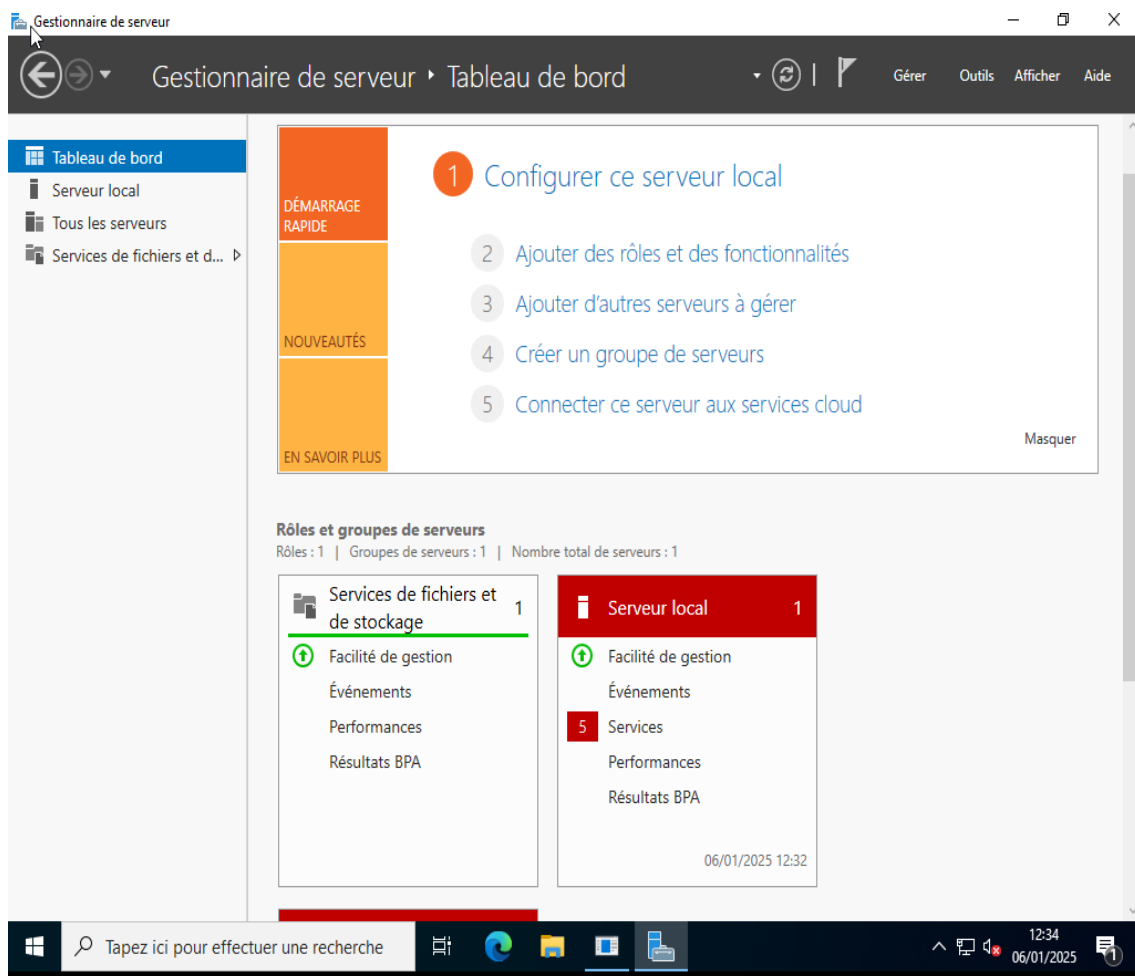


Figure 2



2. Sélection de **Ajouter des rôles et fonctionnalités**.

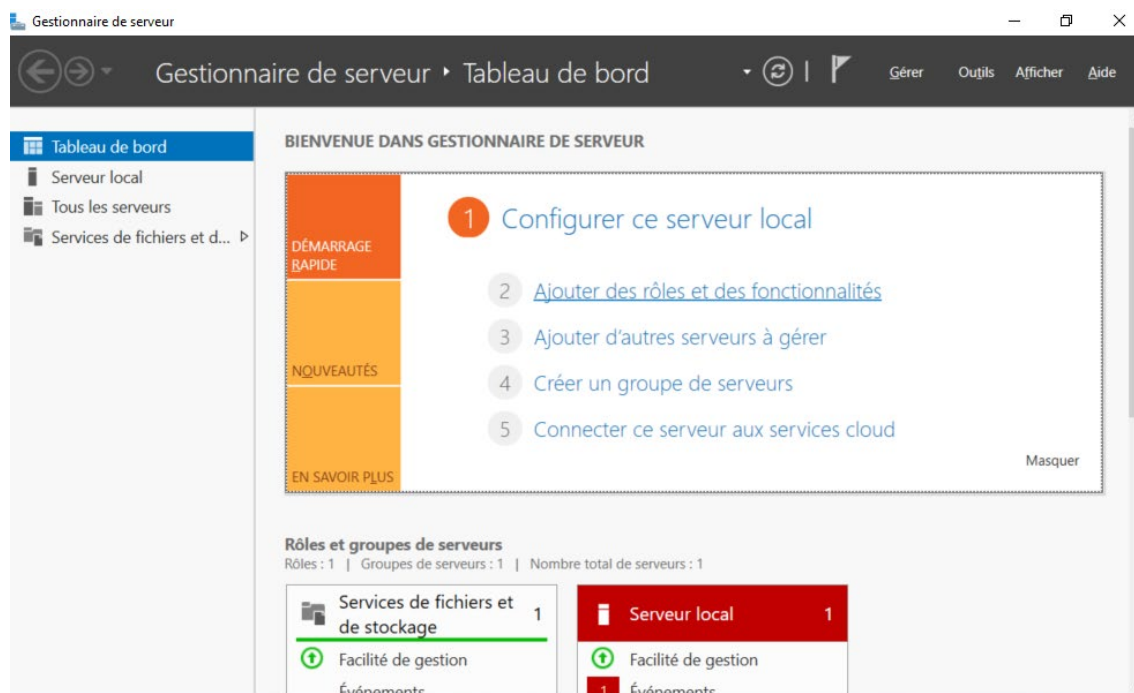


Figure 3



3. Choix du rôle **Active Directory Domain Services (ADDS)** et finalisation de l'installation.

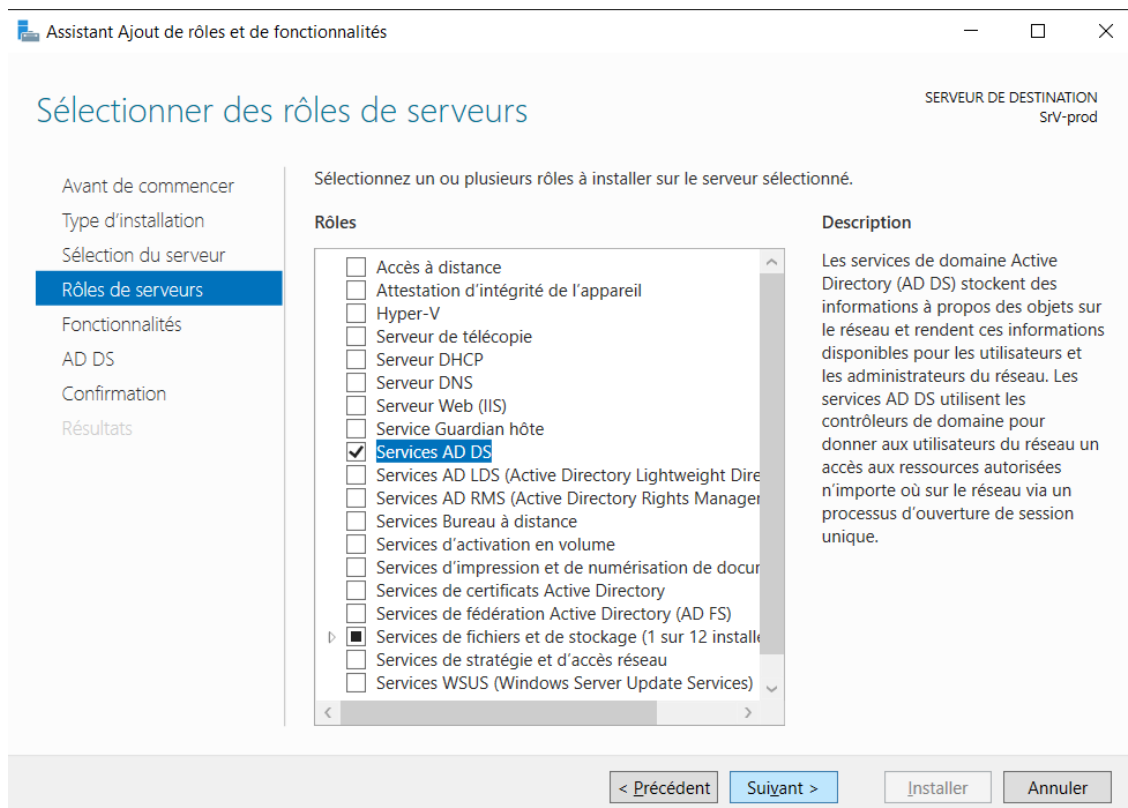


Figure 4

5.1.1.2 Création du domaine Active Directory et promouvoir ce serveur en contrôleur de domaine.

Rappel :

Un domaine, en informatique, est une structure logique utilisée pour regrouper et gérer des ressources réseau sous une même autorité. Dans les environnements Windows, un domaine Active Directory (AD), introduit par Microsoft en 1999, permet l'authentification centralisée et la gestion des utilisateurs, ordinateurs et politiques de sécurité. Il repose sur des composants comme le contrôleur de domaine (DC) (serveur d'authentification), LDAP (protocole d'annuaire), Kerberos (authentification sécurisée), Group Policy (gestion des stratégies) et DNS (résolution des noms). Grâce à son administration centralisée et sa scalabilité, un domaine est essentiel pour les entreprises, assurant la sécurité, la gestion des accès et la cohérence des configurations sur un réseau.

Après l'installation du rôle ADDS, j'ai promu le serveur en contrôleur de domaine et créé le domaine sistr.local.



Étapes suivies :

1. Lancement de l'**Assistant de promotion de contrôleur de domaine**.

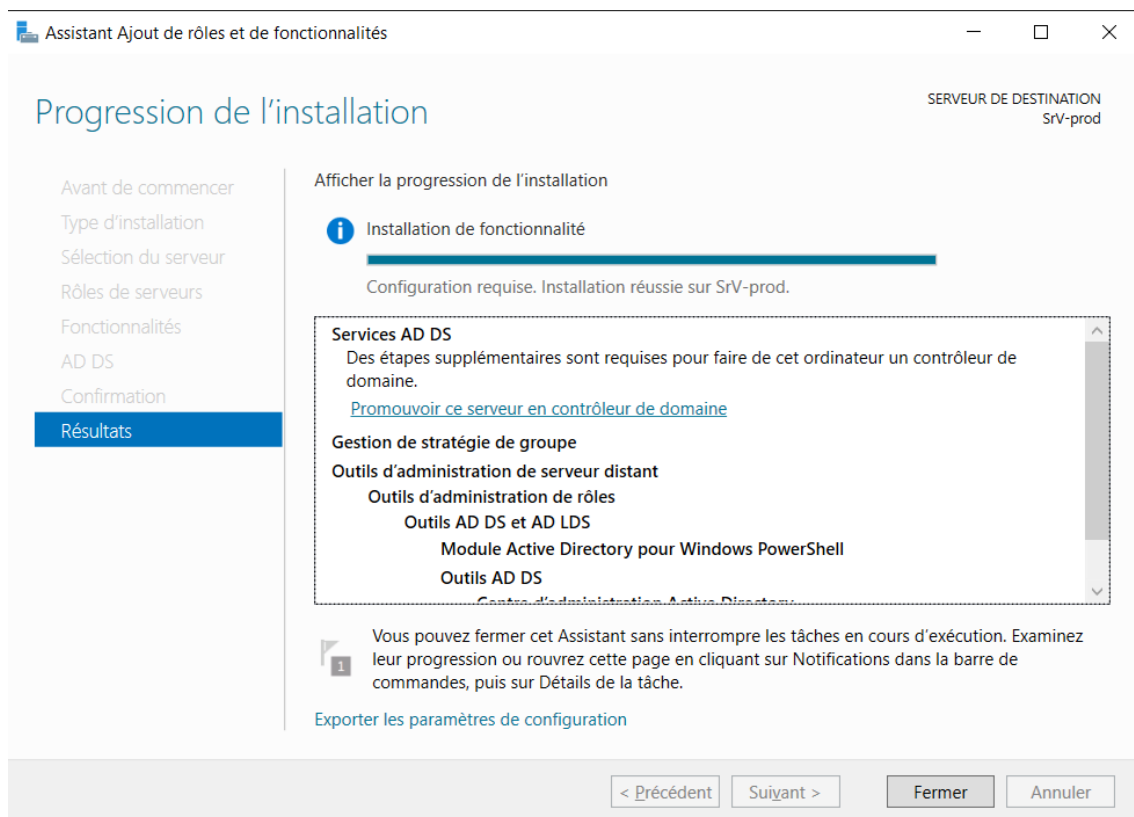


Figure 5



2. Sélection de l'option pour **créer un nouveau domaine dans une nouvelle forêt**. Et Configuration du nom du domaine **SISR.local**.

Assistant Configuration des services de domaine Active Directory

Configuration de déploiement

SERVEUR CIBLE
SrV-prod

Configuration de déploiement

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

☐ Ajouter un contrôleur de domaine à un domaine existant

☐ Ajouter un nouveau domaine à une forêt existante

☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

[En savoir plus sur les configurations de déploiement](#)

< Précédent

Suivant >

Installer

Annuler

Figure 6



3. Finalisation de la promotion et redémarrage du serveur pour appliquer les changements.

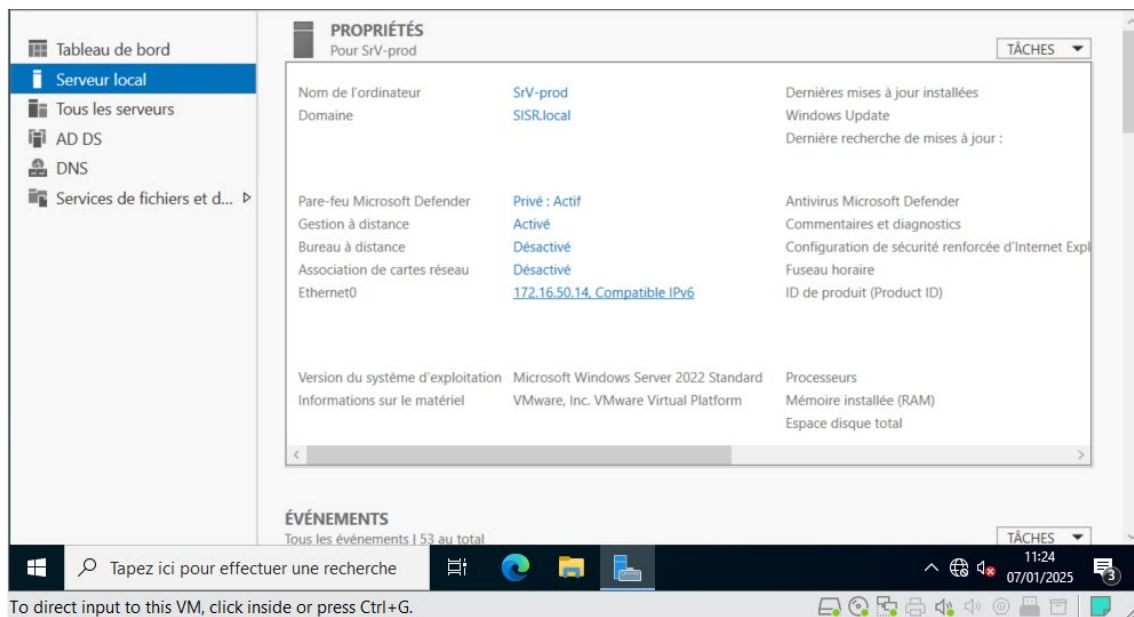


Figure 7

5.1.1.3 Configuration du serveur DNS

Rappel :

Le DNS (Domain Name System), créé en 1983 par Paul Mockapetris, est un système permettant de traduire les noms de domaine lisibles par les humains (ex. www.example.com) en adresses IP compréhensibles par les machines. Il fonctionne sur un modèle hiérarchique et distribué, avec des serveurs racine, des serveurs TLD (Top-Level Domain) et des serveurs faisant autorité. Le DNS utilise principalement le protocole UDP sur le port 53 pour les requêtes rapides et TCP pour les transferts de zones. Il est essentiel pour la navigation sur Internet et joue un rôle clé dans les services réseau, y compris l'Active Directory, où il est utilisé pour localiser les contrôleurs de domaine.

Une fois le domaine créé, j'ai configuré le serveur en tant que serveur **DNS** pour qu'il puisse résoudre les noms de domaine du réseau. Le serveur DNS est une partie intégrante de l'Active Directory, car il permet la résolution des noms des machines du domaine.



Étapes suivies :

1. Ouverture du **Gestionnaire de serveur**.

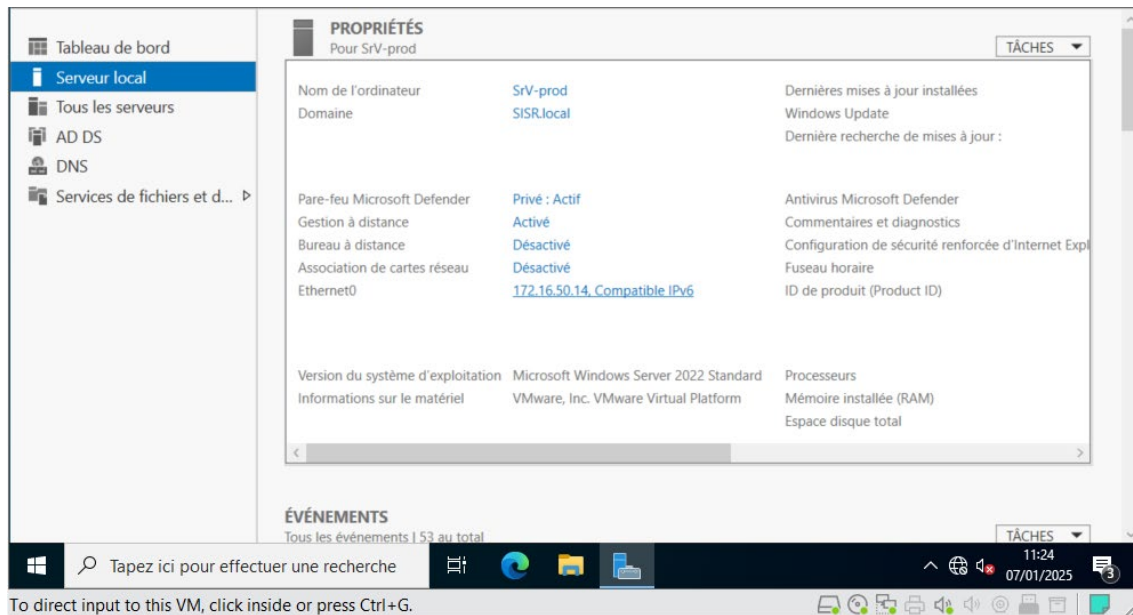


Figure 8

2. Sélection **DNS** puis Gestionnaire DNS.

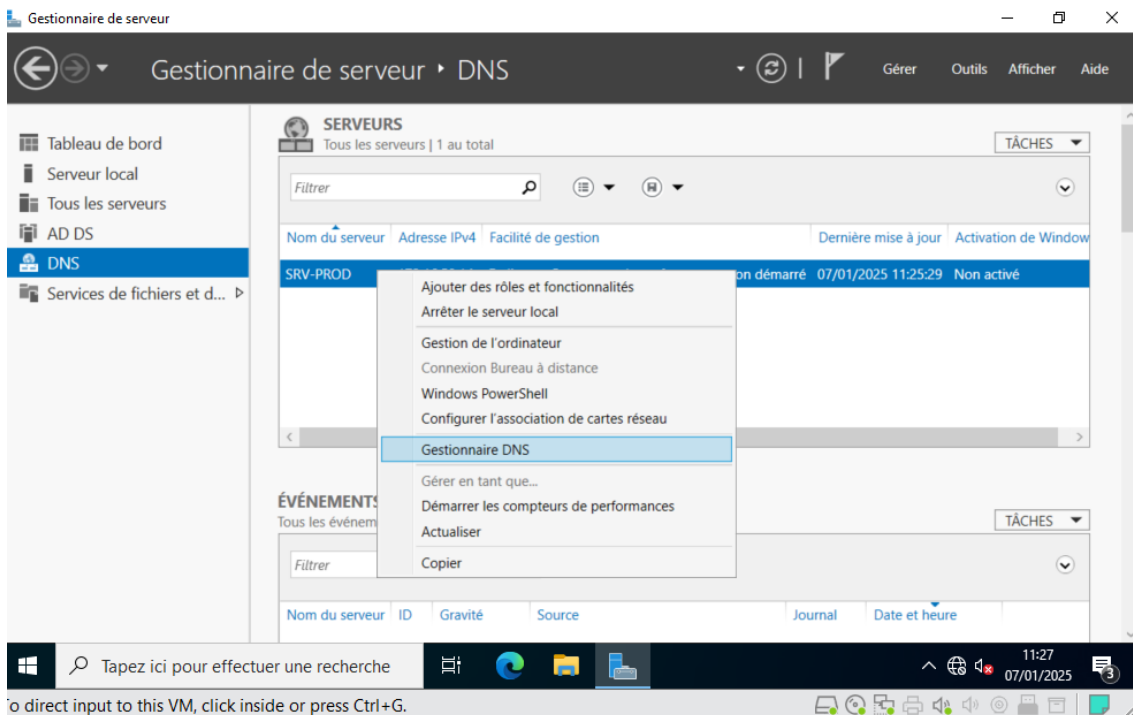


Figure 9



3. Configuration de la **zone de recherche indirecte** pour **SISR.local**.

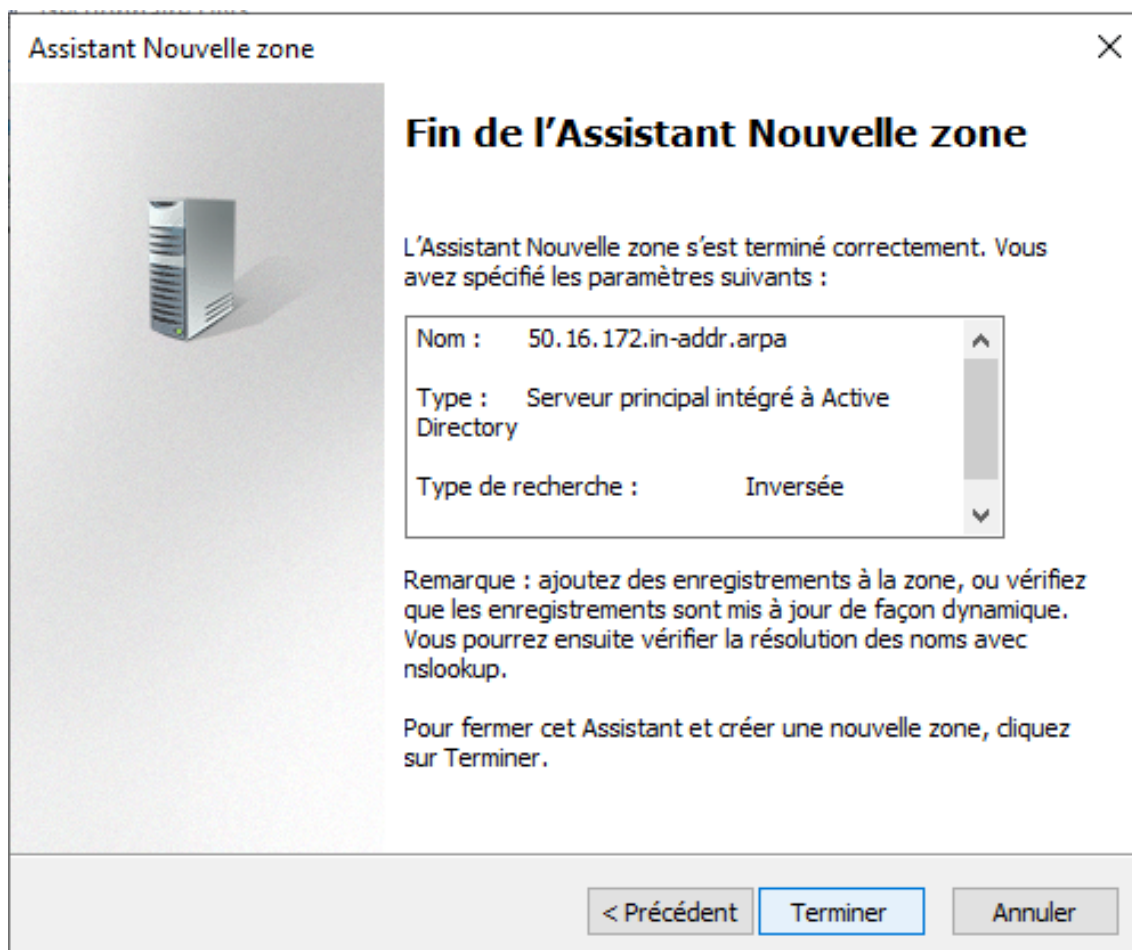


Figure 10



4. Configuration de la **zone de recherche directe** pour **form.local**.

Propriétés de : srv-prod

Hôte local (A) Sécurité

Hôte (utilise le domaine parent si ce champ est vide) :
srv-prod

Nom de domaine pleinement qualifié (FQDN) :
srv-prod.SISR.local

Adresse IP :
172.16.50.14

☒ Mettre à jour l'enregistrement de pointeur (PTR) associé

OK Annuler Appliquer

Figure 11

5. ? Vérification des enregistrements SRV nécessaires pour le bon fonctionnement de l'Active Directory.

```
Sélection Administrateur : Invite de commandes - nslookup
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>nslookup
Serveur par défaut :  srv-prod.SISR.local
Address:  172.16.50.14
```

Figure 12



5.1.1.4 Gestion des utilisateurs, groupes et unités d'organisation via PowerShell.

Rappel :

Le PowerShell, créé par Microsoft en 2006, est un shell et un langage de script basé sur .NET, conçu pour l'automatisation et l'administration des systèmes Windows. Il utilise des cmdlets comme Get-Command (liste des commandes), Get-Help (aide sur une commande), Get-Process (affichage des processus), Set-ExecutionPolicy (gestion de la politique d'exécution des scripts) et Invoke-Command (exécution à distance). Grâce à son système de pipelines et sa prise en charge des scripts avancés, il est essentiel pour l'administration de Windows Server, Active Directory et Azure, offrant un contrôle puissant sur les infrastructures IT.

Après avoir configuré le rôle **Active Directory Domain Services (ADDS)**, créé le domaine et configuré le serveur **DNS**, j'ai utilisé **PowerShell** pour automatiser la gestion des utilisateurs, des groupes et des unités d'organisation (OU).



Toutes les commandes PowerShell nécessaires à la gestion de l'Active Directory ont été exécutées dans une seule session PowerShell.

```
1 #Creation d'une unité organisation (OU)
2 New-ADOrganizationalUnit -Name "DIRECTION" -Path "DC=sisr,DC=local"
3 -ProtectedFromAccidentalDeletion $true -Server "srv-prod.sisr.local"
4
5
6 #Creation d'un utilisateur et ajout de l'utilisateur dans l'OU
7 New-ADUser -Name "Adobi ba" -GivenName "Adobi" -Surname "ba"
8 -SamAccountName "A.ba" -UserPrincipalName "A.ba@sisr.local"
9 -Path "OU=DIRECTION,DC=sisr,DC=local"
10 [-AccountPassword (ConvertTo-SecureString "Respons11!@?,"
11 [-AsPlainText -Force] -Enabled $true -EmailAddress "ado.ba@sisr.local"
12
13
14 #Creation d'un Groupe
15 New-ADGroup -Name "Direction" -SamAccountName "Direction"
16 -GroupCategory "security" -GroupScope "Global" -Path "OU=DIRECTION,DC=sisr,DC=local"
17
18
19 #Ajout de l'utilisateur dans le groupe
20 Add-ADGroupMember -Identity "Direction" -Members "A.ba"
```

```
PS C:\Users\Administrateur> #Creation d'une unité organisation (OU)
New-ADOrganizationalUnit -Name "DIRECTION" -Path "DC=sisr,DC=local" -ProtectedFromAccidentalDeletion $true -Server "srv-prod.sisr.local"

#Creation d'un utilisateur et ajout de l'utilisateur dans l'OU
New-ADUser -Name "Adobi ba" -GivenName "Adobi" -Surname "ba" -SamAccountName "A.ba" -UserPrincipalName "A.ba@sisr.local" -Path "OU=DIRECTION,DC=sisr,DC=local" [-AccountPassword (ConvertTo-SecureString "Respons11!@?," [-AsPlainText -Force] -Enabled $true -EmailAddress "ado.ba@sisr.local"

#Creation d'un Groupe
New-ADGroup -Name "Direction" -SamAccountName "Direction" -GroupCategory "security" -GroupScope "Global" -Path "OU=DIRECTION,DC=sisr,DC=local"

#Ajout de l'utilisateur dans le groupe
Add-ADGroupMember -Identity "Direction" -Members "A.ba"

PS C:\Users\Administrateur>
```

Figure 13



5.1.1.4.1 Vérification des enregistrements SRV nécessaires pour le bon fonctionnement de l'Active Directory.

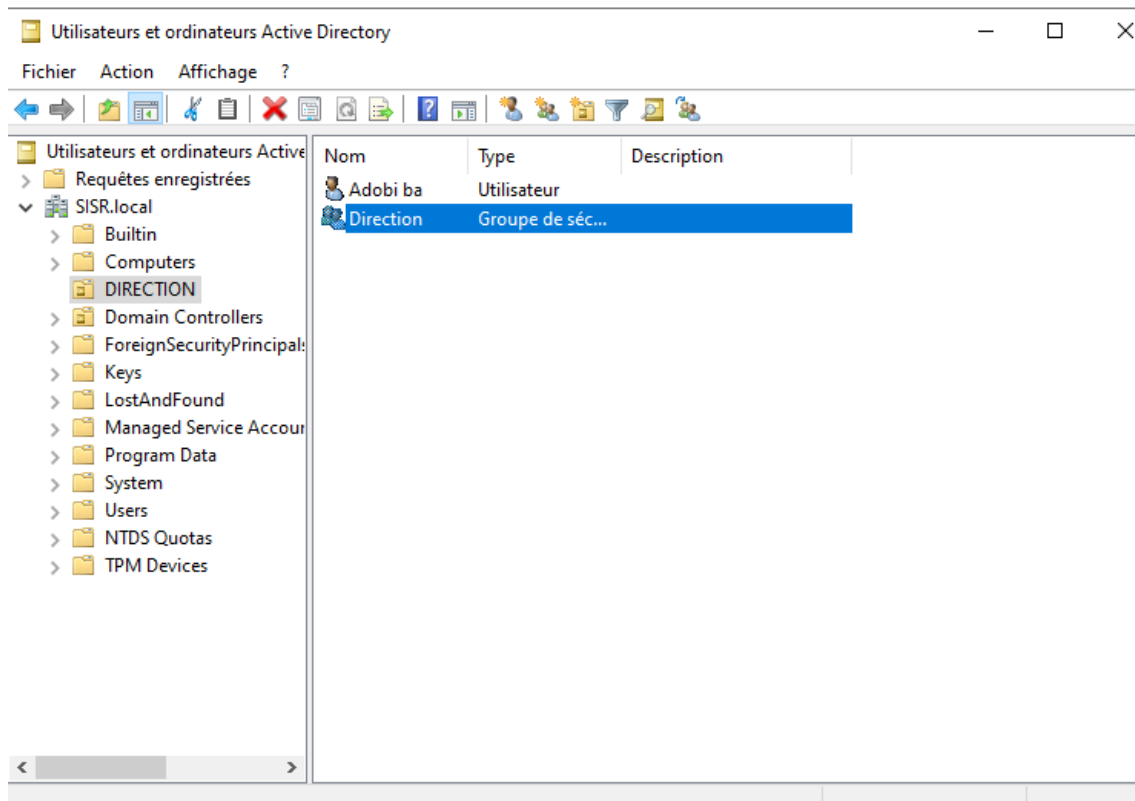


Figure 14



5.1.1.4.2 Mise en place des GPO pour le lecteur mappé.

Rappel :

Un Group Policy Object (GPO) est un ensemble de règles et de configurations appliquées aux utilisateurs et aux ordinateurs d'un domaine Active Directory. Il permet d'automatiser la gestion des stratégies de sécurité, des paramètres réseau, des logiciels et des restrictions sur les postes clients.

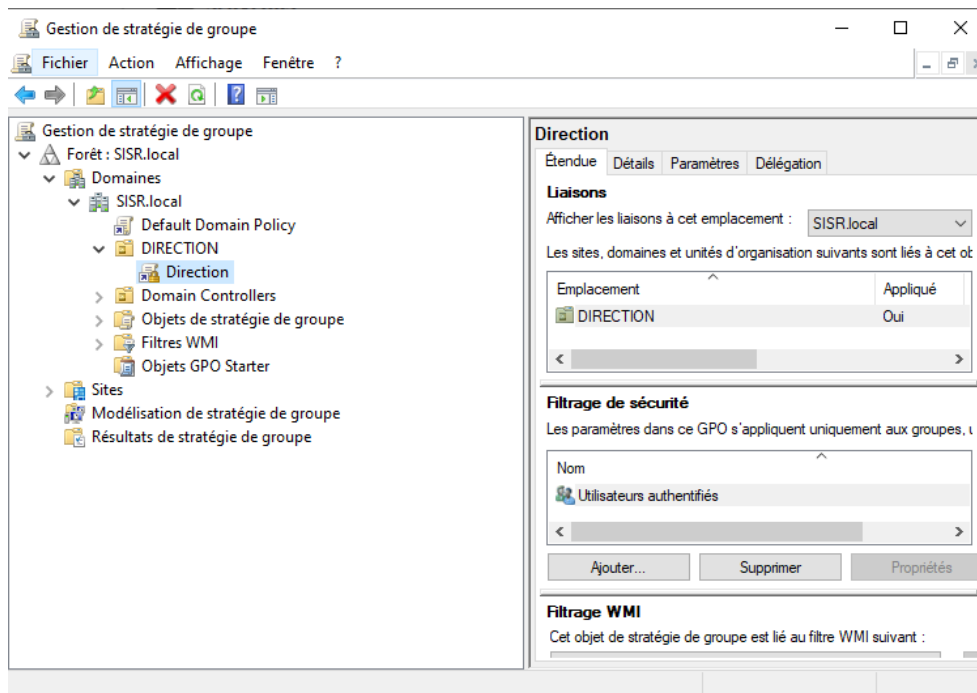
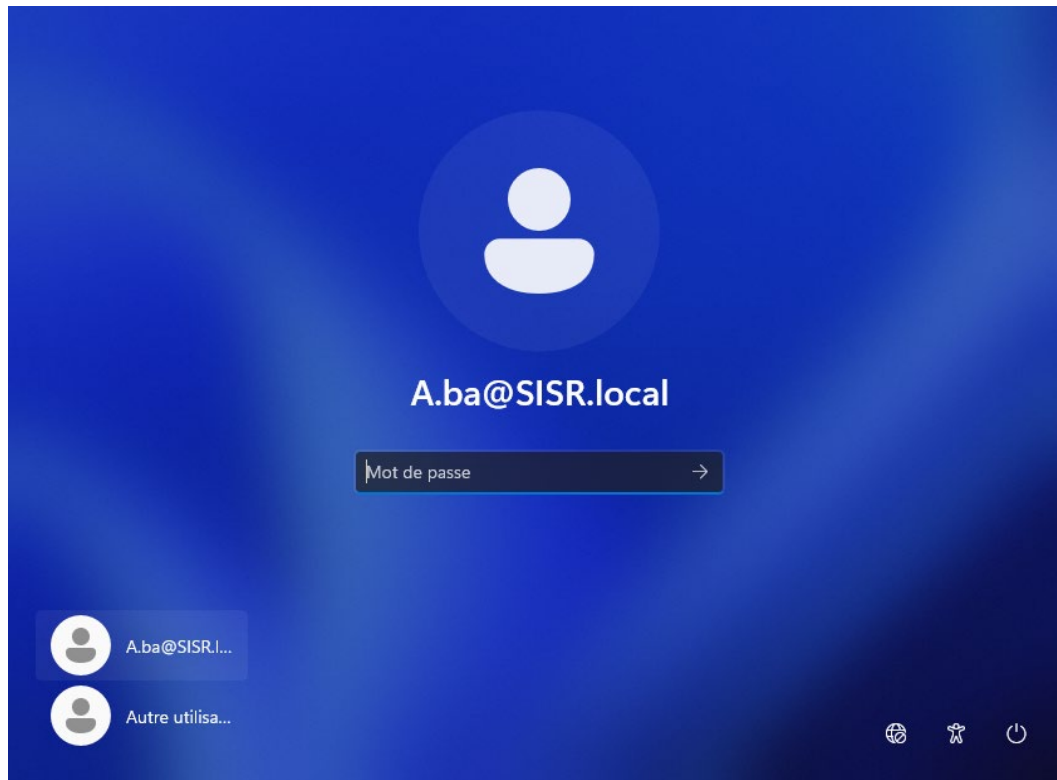


Figure 15



5.1.1.4.3 Installation des Windows 10 et 11

❖ Windows 11.



Le **poste Windows 11**, intégré au réseau local (LAN), répond aux enjeux du projet en matière de **gestion centralisée des utilisateurs et de sécurité des accès**. En étant membre du domaine **SISR.local**, il permet d'appliquer les **politiques de groupe (GPO)** définies par l'Active Directory, garantissant ainsi un **contrôle strict des permissions et des ressources**. Ce poste illustre la mise en place d'une infrastructure où les employés peuvent travailler de manière sécurisée tout en accédant aux services essentiels, tels que les **partages de fichiers, les applications métiers et les services réseau**. Il contribue également à la politique de **sécurisation des postes clients**, en testant l'application des règles de sécurité et en simulant l'expérience d'un utilisateur classique du réseau interne.



❖ Window10



Le **poste Windows 10**, situé en dehors du réseau local (WAN), incarne l'enjeu du **travail à distance sécurisé et de l'administration externe**. Grâce à un **VPN (Virtual Private Network)** configuré via **PfSense**, il assure une connexion sécurisée au réseau interne, prévenant ainsi les risques liés aux accès non autorisés. Ce poste est essentiel pour tester **l'efficacité des solutions de cybersécurité mises en place**, notamment la robustesse de l'authentification et le chiffrement des communications. De plus, l'accès via **Remote Desktop Protocol (RDP)** permet à l'utilisateur distant de **se connecter à sa session**, garantissant ainsi une **continuité des opérations** même en cas d'indisponibilité sur site.



5.1.2 CONFIGURATION DE PFSENSE

Rappel :

pfSense est un système d'exploitation open-source basé sur FreeBSD, conçu pour fonctionner comme un pare-feu et un routeur réseau, offrant une administration centralisée et une grande flexibilité. Il intègre des fonctionnalités avancées telles que le filtrage de paquets avec Packet Filter (pf), la gestion des VPN (OpenVPN, IPsec, WireGuard), la segmentation réseau avec VLANs, un portail captif pour l'authentification des utilisateurs, ainsi qu'un IDS/IPS (Snort, Suricata) pour détecter et prévenir les intrusions. Grâce à son support du load balancing, de la haute disponibilité (CARP, pfSync) et de la surveillance réseau (Zabbix, Prometheus), pfSense assure une gestion sécurisée et évolutive des réseaux, en s'adaptant aussi bien aux besoins des entreprises qu'aux infrastructures domestiques exigeantes.

Dans ce projet, la mise en place et la configuration de pfSense ont été réalisées de manière autonome. Le processus a suivi les étapes suivantes :

- ❖ Mise en place du pare-feu avec deux interfaces : WAN (Internet) et LAN (Réseau local).
- ❖ Configuration de l'authentification LDAP avec Active Directory.
- ❖ Génération des certificats auto-signés pour sécuriser OpenVPN.
- ❖ Installation et configuration d'OpenVPN pour l'accès distant sécurisé.
- ❖ Exportation et test du VPN sur Windows 10.

5.1.2.1 Mise en place du pare-feu avec deux interfaces : WAN et LAN

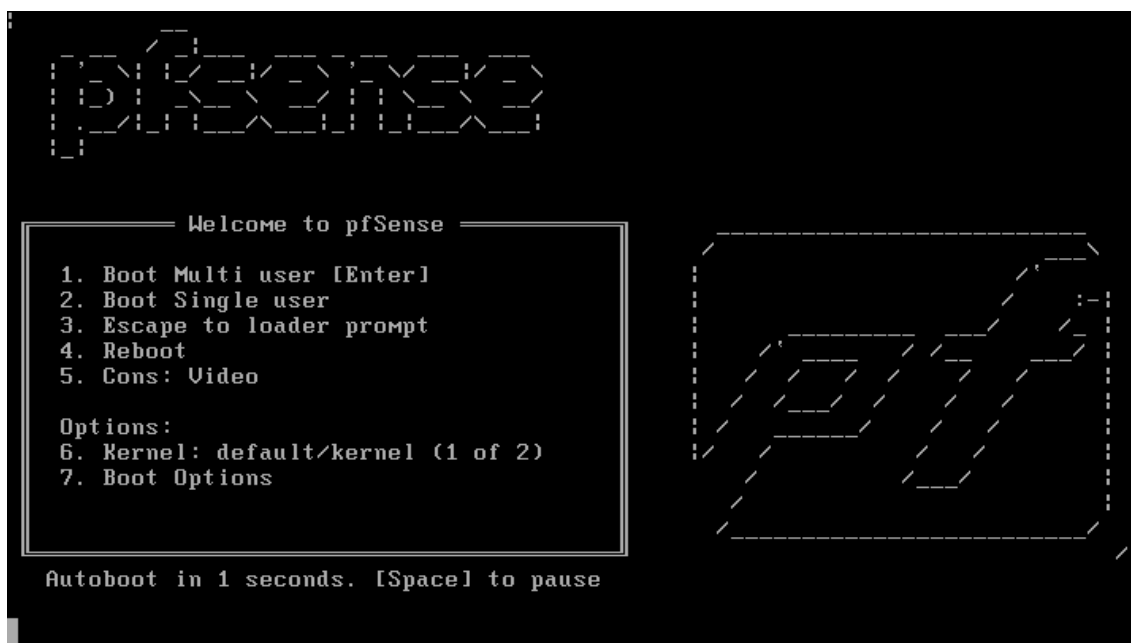


Figure 16



Étapes suivies :

1. Configuration initiale des interfaces WAN et LAN en attribuant des adresses IP statiques.

La première étape a été l'installation et la configuration de pfSense avec deux interfaces réseau : une pour la connexion Internet (WAN) et une pour le réseau interne (LAN).

```
Starting CRON... done.
Starting package OpenVPN Client Export Utility...done.
pfSense 2.7.2-RELEASE amd64 20240304-1953
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 4ffc8d5c02880a32ce46

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.52/24
LAN (lan)      -> em1      -> v4: 172.16.50.13/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Figure 17



2. Accès à l'interface web d'administration via une adresse IP par défaut

pfSense Logo

Login to pfSense

SIGN IN

admin

.....

SIGN IN

Figure 18

5.1.2.2 Configuration de l'authentification LDAP avec Active Directory

Pour centraliser l'authentification des utilisateurs, pfSense a été configuré pour utiliser LDAP en lien avec Active Directory.

Étapes suivies :

1. Accès à l'interface web de pfSense et navigation vers System > User Manager > Authentication Servers.

System / User Manager / Authentication Servers

Users Groups Settings Authentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
Local Database	Local Database	pfSense	

+ Add

Figure 19



2. Ajout d'un nouveau serveur d'authentification LDAP avec les paramètres du contrôleur de domaine AD.

[System](#) / [User Manager](#) / [Authentication Servers](#) / [Edit](#) ?

[Users](#) [Groups](#) [Settings](#) [Authentication Servers](#)

Server Settings

Descriptive name

Srv-pro

Type

LDAP

LDAP Server Settings

Hostname or IP address

172.16.50.14

NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value

389

Transport

Standard TCP

Peer Certificate Authority

Global Root CA List

This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version

3

Server Timeout

25

Timeout for LDAP operations (seconds)

Search scope

Level

One Level

Base DN

DC=SISR,DC=local

Authentication containers

OU=DIRECTION,DC=sisr,DC=local

[Select a container](#)

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers

Extended query

☐ Enable extended query



Bind anonymous

☐ Use anonymous binds to resolve distinguished names

Bind credentials

SISR\A.ba

User naming attribute

samAccountName

Group naming attribute

cn

Group member attribute

memberOf

RFC 2307 Groups

☐ LDAP Server uses RFC 2307 style group membership

RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class

posixGroup

Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN

If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

UTF8 Encode

☐ UTF8 encode LDAP parameters before sending them to the server.

Required to support international characters, but may not be supported by every LDAP server.

Username Alterations

☐ Do not strip away parts of the username after the @ symbol

e.g. user@host becomes user when unchecked.

Allow unauthenticated bind

☐ Allow unauthenticated bind

Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

Save

UsersGroupsSettingsAuthentication Servers

Authentication Servers

Server Name	Type	Host Name	Actions
Srv-pro	LDAP	172.16.50.14	
Local Database		pfSense	

+

 Add

Figure 20

3. Test de la connexion LDAP pour s'assurer de la communication avec Active Directory.

LDAP settings

Test results

Attempting connection to	172.16.50.14	OK
Attempting bind to	172.16.50.14	OK
Attempting to fetch Organizational Units from	172.16.50.14	OK
Organization units found OU=DIRECTION,DC=SISR,DC=local OU=Domain Controllers,DC=SISR,DC=local CN=Users,DC=SISR,DC=local		

Figure 21



5.1.2.3 Génération des certificats auto-signés pour sécuriser OpenVPN

Afin d'assurer une connexion sécurisée via VPN, des certificats auto-signés ont été générés pour OpenVPN.

Étapes suivies :

1. Accès à l'interface web de pfSense et navigation vers System > Certificate Manager.

The screenshot shows the pfSense web interface for the Certificate Manager. The breadcrumb trail is 'System / Certificate / Authorities'. The 'Authorities' tab is selected. Below the breadcrumb is a search bar with a 'Search term' input field, a 'Both' dropdown, and 'Search' and 'Clear' buttons. Below the search bar is a table titled 'Certificate Authorities'. The table has columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. The table is currently empty, and there is a green '+ Add' button at the bottom right.

Figure 22

2. Création d'une autorité de certification (CA) interne.

The screenshot shows the pfSense web interface for the Certificate Manager. The breadcrumb trail is 'System / Certificate / Authorities'. The 'Authorities' tab is selected. Below the breadcrumb is a search bar with a 'Search term' input field, a 'Both' dropdown, and 'Search' and 'Clear' buttons. Below the search bar is a table titled 'Certificate Authorities'. The table has columns: Name, Internal, Issuer, Certificates, Distinguished Name, In Use, and Actions. The table contains one entry: 'VPN_Root_CA' with a checkmark in the 'Internal' column, 'self-signed' in the 'Issuer' column, '3' in the 'Certificates' column, and 'ST=SISR, O=webitech, L=Paris, CN=local, C=FR' in the 'Distinguished Name' column. The 'In Use' column has an information icon. The 'Actions' column has icons for edit, delete, and refresh. Below the table is a green '+ Add' button.

Figure 23



3. Génération d'un certificat de serveur pour OpenVPN.

















<div> <div>Authorities</div> <div>Certificates</div> <div>Certificate Revocation</div> </div>				
Search				
Search term		Both	Search	Clear
Enter a search string or *nix regular expression to search certificate names and distinguished names.				
Certificates				
Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (67cc3fda00f50) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-67cc3fda00f50 Valid From: Sat, 08 Mar 2025 13:02:18 +0000 Valid Until: Fri, 10 Apr 2026 13:02:18 +0000	webConfigurator	   
VPN_Root_CA.certificate User Certificate CA: No Server: No	VPN_Root_CA	ST=SISR, O=webitech, L=Paris, CN=local, C=FR Valid From: Sat, 08 Mar 2025 13:28:04 +0000 Valid Until: Tue, 06 Mar 2035 13:28:04 +0000		   
VPN_Root_CA.certificatedd Server Certificate CA: No Server: Yes	VPN_Root_CA	ST=SISR, O=webitech, L=Paris, CN=local, C=FR Valid From: Sat, 08 Mar 2025 13:29:25 +0000 Valid Until: Tue, 06 Mar 2035 13:29:25 +0000	OpenVPN Server	   
sysbotVpn User Certificate CA: No Server: No	VPN_Root_CA	ST=SISR, O=webitech, L=Paris, CN=SysBot, C=FR Valid From: Sat, 08 Mar 2025 13:37:23 +0000 Valid Until: Tue, 06 Mar 2035 13:37:23 +0000	User Cert	   

Figure 24



5.1.2.4 Installation et configuration d'OpenVPN pour l'accès distant sécurisé

L'installation et la configuration d'OpenVPN ont été effectuées pour permettre un accès distant sécurisé aux ressources du réseau interne.

Étapes suivies :

1. Accès à VPN > OpenVPN et lancement de l'assistant de configuration sélection du mode serveur et choix des certificats générés précédemment.

The screenshot shows the 'OpenVPN Servers' configuration page. It includes tabs for Servers, Clients, Client Specific Overrides, Wizards, and Client Export. The 'Servers' tab is active, showing a table with one server configuration. The table has columns for Interface, Protocol / Port, Tunnel Network, Mode / Crypto, Description, and Actions. The server is named 'WAN', uses 'UDP4 / 1194 (TUN)', and has a tunnel network of '10.10.10.0/24'. The mode is 'Remote Access (SSL/TLS + User Auth)' with various ciphers and digests listed. An 'Add' button is at the bottom right.

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	10.10.10.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	Tunnel	[Edit] [Clone] [Delete]

+ Add

Figure 25

2. Ajout des règles de pare-feu pour autoriser le trafic OpenVPN.

❖ Interface OPVPN : Configuration des règles de pare-feu sur l'interface OpenVPN

The screenshot shows the 'Firewall Rules' configuration page for the 'OpenVPN' interface. It includes tabs for Floating, WAN, LAN, and OpenVPN. The 'OpenVPN' tab is active, showing a table with two rules. The table has columns for States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. The first rule is 'Autoriser le RDP vers Windows 11' and the second is 'Bloquer tous le trafic dans le tunnel'. An 'Add' button is at the bottom right.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> [Green Check]	0/0 B	IPv4	*	*	172.16.50.22	3389 (MS RDP)	*	none	Autoriser le RDP vers Windows 11	[Anchor] [Edit] [Clone] [Delete]
<input type="checkbox"/> [Yellow Hand]	0/0 B	IPv4	*	*	*	*	*	none	Bloquer tous le trafic dans le tunnel	[Anchor] [Edit] [Clone] [Delete]

[Add] [Add] [Delete] [Toggle] [Copy] [Save] [Separator]

Figure 26



❖ Interface LAN : Configuration des règles de pare-feu sur l'interface LAN pour OpenVPN

Firewall / Rules / LAN

Floating WAN LAN OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 4/1.81 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
□ ✓ 0/0 B	IPv4 UDP	*	*	*	1194 (OpenVPN)	*	none		Autorisation du port UDP dans le LAN	🔗 📄 🗑️
□ ✓ 0/0 B	IPv4 TCP	*	*	*	3389 (MS RDP)	*	none		Autorisation du port UDP	🔗 📄 🗑️
□ ✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 📄 🗑️
□ 🖐️ 0/160 KiB	IPv4 *	*	*	*	*	*	none		Bloquer tous le trafic dans le LAN	🔗 📄 🗑️

↑ Add ↓ Add 🗑️ Delete ⚙️ Toggle 📄 Copy 💾 Save ➕ Separator

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Figure 27



❖ Interface WAN : Configuration des règles de pare-feu sur l'interface WAN pour OpenVPN

Floating WAN LAN OpenVPN											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		Autoriser le VPN	
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	👉 0/0 B	IPv4 *	*	*	172.16.50.0/24	*	*	none		Bloquer tous le trafic dans le vers le LAN	
Add Add Delete Toggle Copy Save Separator											

Figure 28

6. TESTS ET VALIDATION

❖ Téléchargement du client OpenVPN depuis l'interface pfSense

OpenVPN Clients		
User	Certificate Name	Export
Certificate with External Auth	VPN_Root_CA_certificate	- Inline Configurations: - Bundled Configurations: - Current Windows Installer (2.6.7-1x001): - Previous Windows Installer (2.5.9-1x601): - Legacy Windows Installers (2.4.12-1x601): - Viscosity (Mac OS X and Windows):

Figure 29



- ❖ Installation du client OpenVPN sur la machine distante

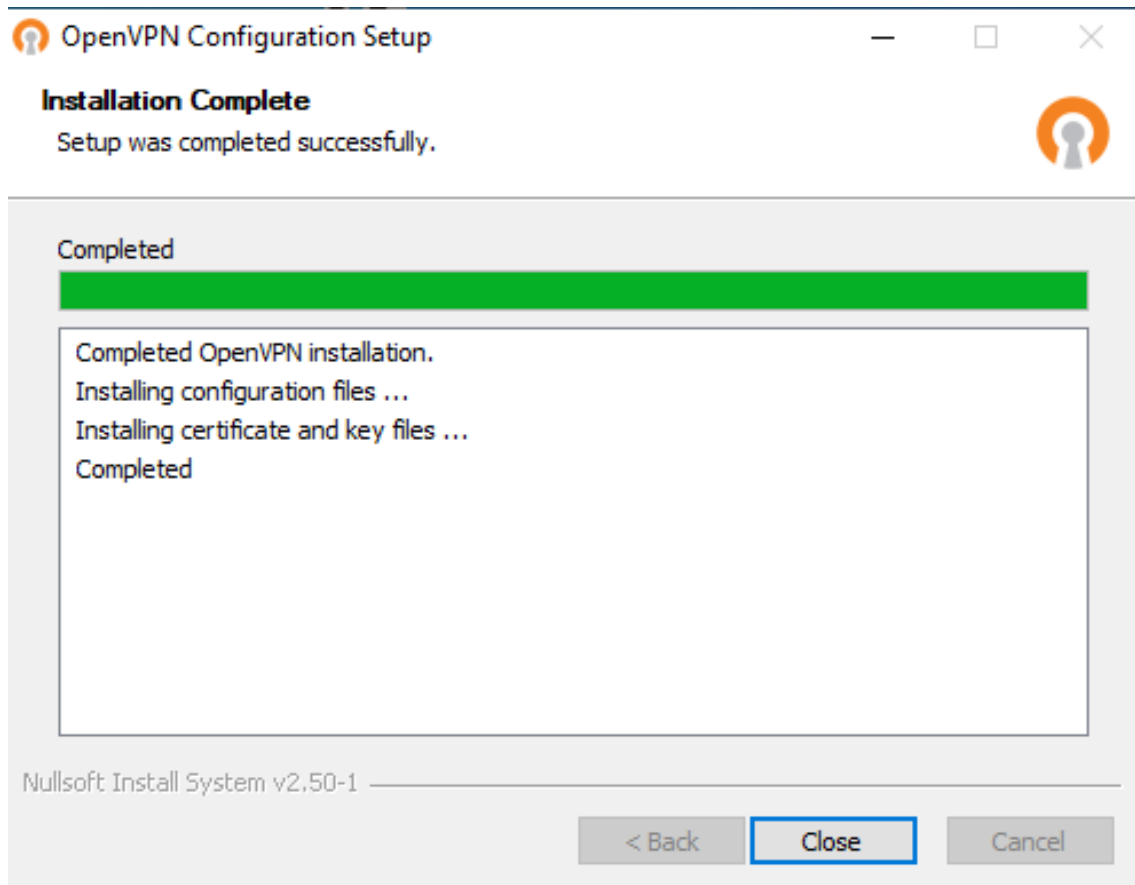


Figure 30



- ❖ Connexion réussie au VPN OpenVPN depuis le client distant

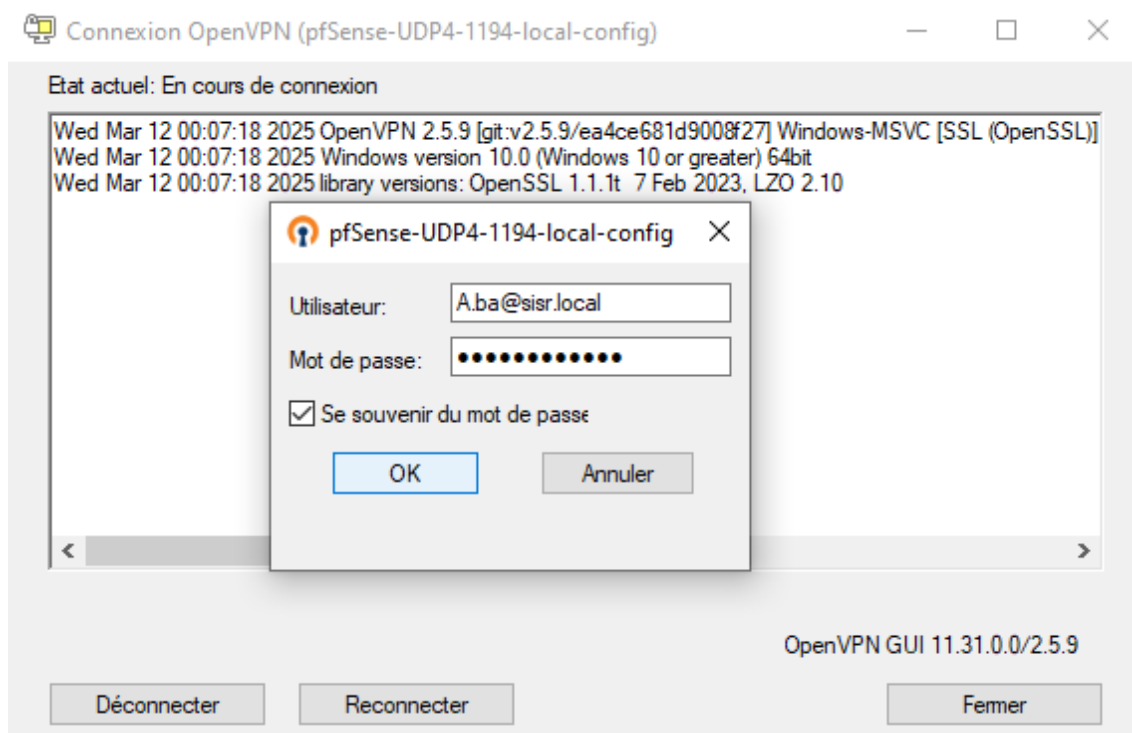


Figure 31



❖ Vérification de l'attribution d'une adresse IP via OpenVPN

```
Sélection C:\Windows\system32\CMD.exe
Microsoft Windows [version 10.0.19044.1288]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\SysBot>ipconfig

Configuration IP de Windows

Carte inconnue OpenVPN Wintun :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet0 :

    Suffixe DNS propre à la connexion. . . : home
    Adresse IPv6. . . . . : 2a01:cb08:c58:c600:44c8:ca2f:ece9:ede1
    Adresse IPv6 temporaire. . . . . : 2a01:cb08:c58:c600:ad50:af6e:b704:38a7
    Adresse IPv6 de liaison locale. . . . : fe80::44c8:ca2f:ece9:ede1%2
    Adresse IPv4. . . . . : 192.168.1.53
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : fe80::1a6a:81ff:fe7c:e8d0%2
                                   192.168.1.1

Carte inconnue OpenVPN TAP-Windows6 :

    Suffixe DNS propre à la connexion. . . : SISR.local
    Adresse IPv6 de liaison locale. . . . : fe80::34ba:7772:1072:857c%26
    Adresse IPv4. . . . . : 10.10.10.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet Connexion réseau Bluetooth :
```

Figure 32

❖ Test de connectivité entre le client distant et les ressources internes



Figure 33



❖ Accès aux ressources internes après connexion au VPN

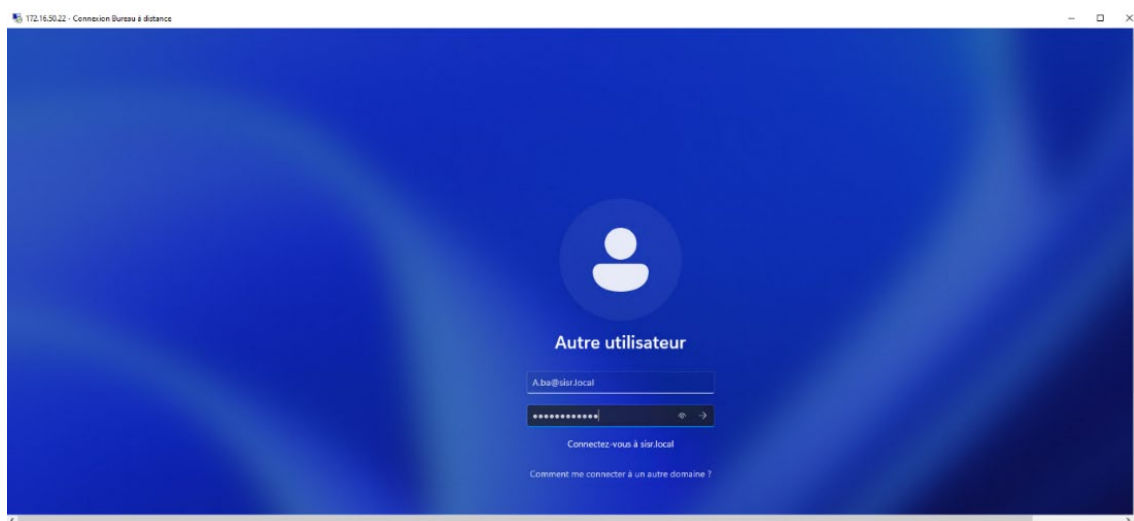


Figure 34



❖ Résumé final du projet – Connexion sécurisée et infrastructure opérationnelle

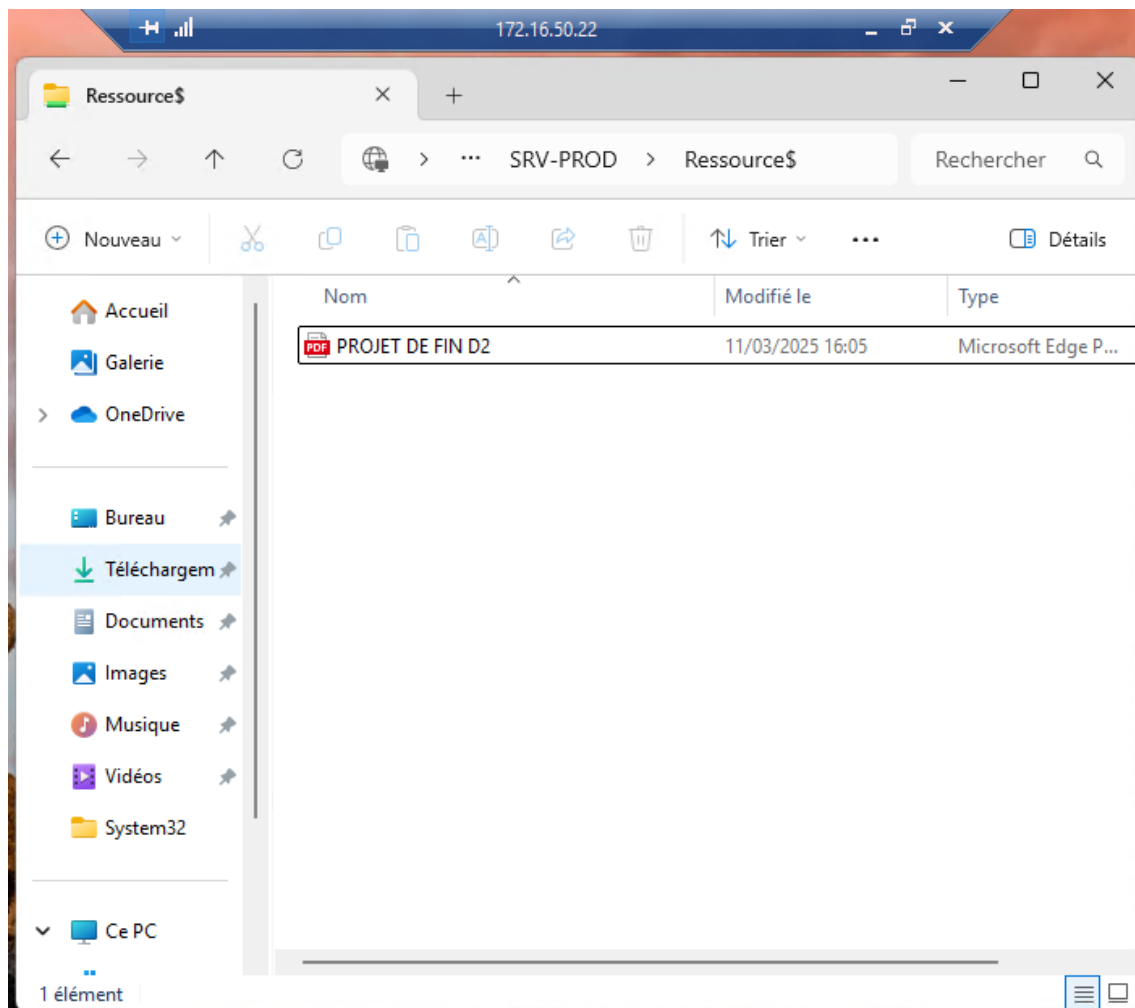


Figure 35

7. PERSPECTIVES D'ÉVOLUTION

- ❖ Supervision et reporting : Intégration de solutions de monitoring.
- ❖ Amélioration de la sécurité : Mise en place d'un système de détection d'intrusion (IDS/IPS).
- ❖ Automatisation avancée : Déploiement d'autres services via PowerShell et Ansible.



8. CONCLUSION

Ce projet m'a permis de relever plusieurs défis, notamment la configuration avancée de pfSense et l'intégration avec Active Directory. J'ai acquis une meilleure maîtrise des outils de gestion des accès et de la sécurité réseau. Pour aller plus loin, l'ajout d'un IDS/IPS et d'une supervision automatisée permettrait d'améliorer encore la sécurité de cette infrastructure.

Les tests effectués ont validé la fonctionnalité des composants, et des améliorations futures peuvent être envisagées, comme l'ajout d'un **système de supervision (Zabbix, Nagios)** ou l'implémentation d'un **IDS/IPS (Snort, Suricata)** pour renforcer encore plus la sécurité du réseau.

En conclusion, cette solution offre une base solide pour les entreprises souhaitant sécuriser leur infrastructure informatique tout en assurant une gestion optimale des accès et des ressources réseau.