10/02/2026

Labo LAN – Infrastructure réseau d'entreprise

Réalisé par Ben Aissa Sofian et Bentatou Ismaïl

Cours SNET 2025 / 2026

GNET

Table des matières

Table des matières

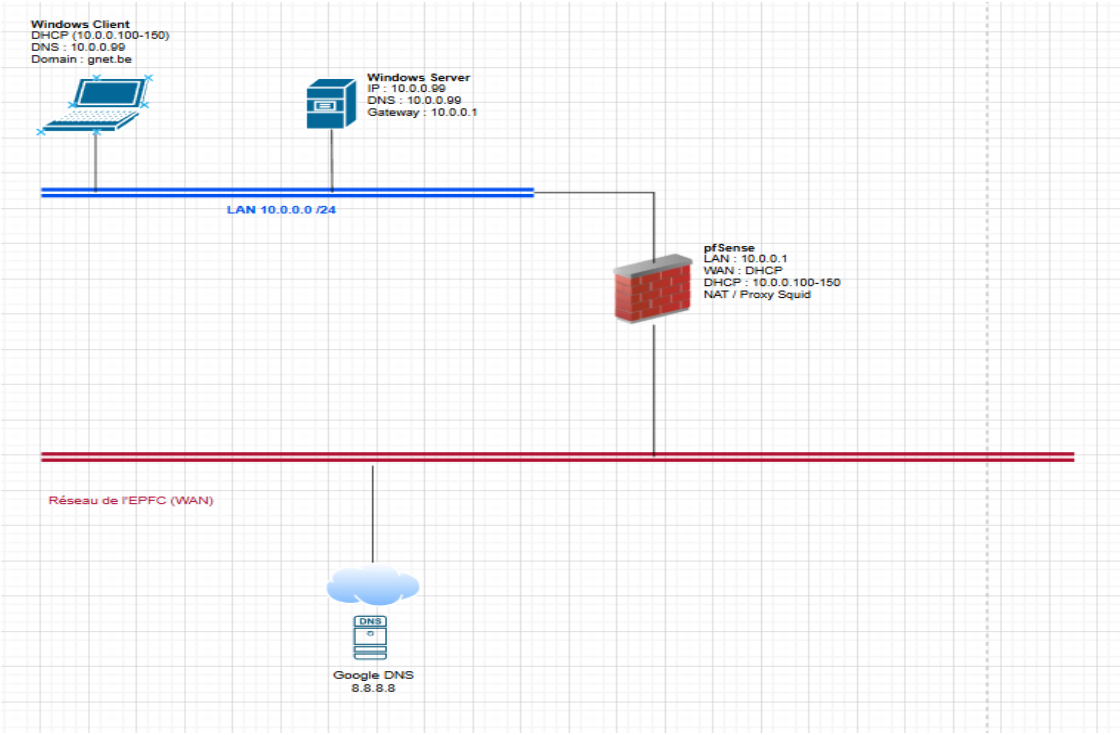
INTRODUCTION

Dans le cadre du cours d'Administration, Gestion et Sécurisation des Réseaux et Services, nous avons réalisé un laboratoire visant à mettre en place une infrastructure réseau d'entreprise fonctionnelle, sécurisée et administrable.

L'objectif principal de ce laboratoire est de comprendre et de manipuler les éléments fondamentaux d'un réseau d'entreprise moderne, à savoir :

- Un firewall,
- Un contrôleur de domaine,
- Un service DNS interne,
- Des clients membres du domaine,
- Un serveur de fichiers,
- Un intranet,
- Un proxy

L'ensemble de l'infrastructure est déployé dans un environnement virtualisé à l'aide de **VirtualBox**, dans un contexte purement pédagogique. Le domaine utilisé est **gnet.be**, conformément aux consignes du laboratoire.



*Le réseau LAN utilise l'adressage **10.0.0.0/24**.*
*Le firewall **pfSense** possède l'adresse **10.0.0.1** et fournit les services **DHCP et NAT**.*

*Le serveur **Windows Server 2019** possède l'adresse **10.0.0.99** et héberge les services **Active Directory, DNS, IIS et File Server**.*

*Les clients **Windows 10** obtiennent automatiquement leur configuration IP via **DHCP**.*

1. PRÉSENTATION DE L'ARCHITECTURE RÉSEAU

Notre architecture réseau est organisée en plusieurs zones distinctes :

- **WAN** : accès vers Internet (réseau externe via réseau de l'école)
- **LAN** : réseau interne de l'entreprise
- **DMZ** : zone intermédiaire destinée à héberger des services exposés (objectif à atteindre pour le prochain laboratoire)

Le firewall **pfSense** est placé en frontal et joue un rôle central dans l'infrastructure :

- Il relie le réseau interne à Internet,
- Il filtre le trafic,
- Il distribue les adresses IP,
- Il fournit des services réseau essentiels.

Le serveur Windows Server 2019 - AD est utilisé comme :

- Contrôleur de domaine (Active Directory),
- Serveur DNS interne,
- Serveur de fichiers,
- Serveur IIS pour l'intranet.

Le **client Windows** représente les postes utilisateurs de l'entreprise et est membre du domaine.

L'utilisation d'un **réseau interne VirtualBox** permet d'isoler complètement l'infrastructure du PC hôte, ce qui reproduit le fonctionnement d'un vrai réseau d'entreprise.

Plan d'adressage IPv4

Afin d'organiser le réseau, nous avons défini un plan d'adressage pour les différentes machines.

LAN : 10.0.0.0 /24

Les adresses utilisées sont les suivantes :

- pfSense (LAN) : 10.0.0.1
- Windows Server 2019 : 10.0.0.10
- Clients Windows : via DHCP

Le serveur DHCP de pfSense distribue les adresses dans la plage suivante :

10.0.0.100 → 10.0.0.150

Ce plan d'adressage permet d'identifier facilement les machines importantes tout en laissant une plage dynamique pour les clients.

2. Mise en place du firewall pfSense

Le firewall **pfSense** a été installé à partir de l'image ISO officielle dans une machine virtuelle VirtualBox.

La machine virtuelle a été configurée avec **trois interfaces réseau** :

- **WAN** configurée en mode *Accès par pont* afin de permettre l'accès à Internet via le réseau de l'ordinateur hôte.
- **LAN** configurée en réseau interne VirtualBox afin de connecter les machines du réseau local.

Après l'installation, les interfaces ont été assignées et configurées.
L'interface **LAN** a reçu l'adresse **10.0.0.1/24**, qui correspond à la passerelle du réseau local.

Le serveur **DHCP** a été activé sur le LAN afin d'attribuer automatiquement des adresses IP aux machines du réseau.
La plage d'adresses configurée est :

10.0.0.100 à 10.0.0.150

pfSense joue plusieurs rôles dans cette architecture :

- **Routeur** entre le LAN et Internet
- **Serveur DHCP** pour l'attribution automatique des adresses IP

- **Serveur DNS / Forwarder**
- **NAT (Network Address Translation)** pour permettre aux machines du LAN d'accéder à Internet via l'adresse WAN

Par défaut, pfSense applique une politique de sécurité restrictive sur l'interface **WAN**, ce qui signifie que les connexions entrantes depuis Internet sont bloquées.

Pour des raisons de sécurité, le port d'accès à l'interface web d'administration a été modifié du port **443** vers le port **8443**.

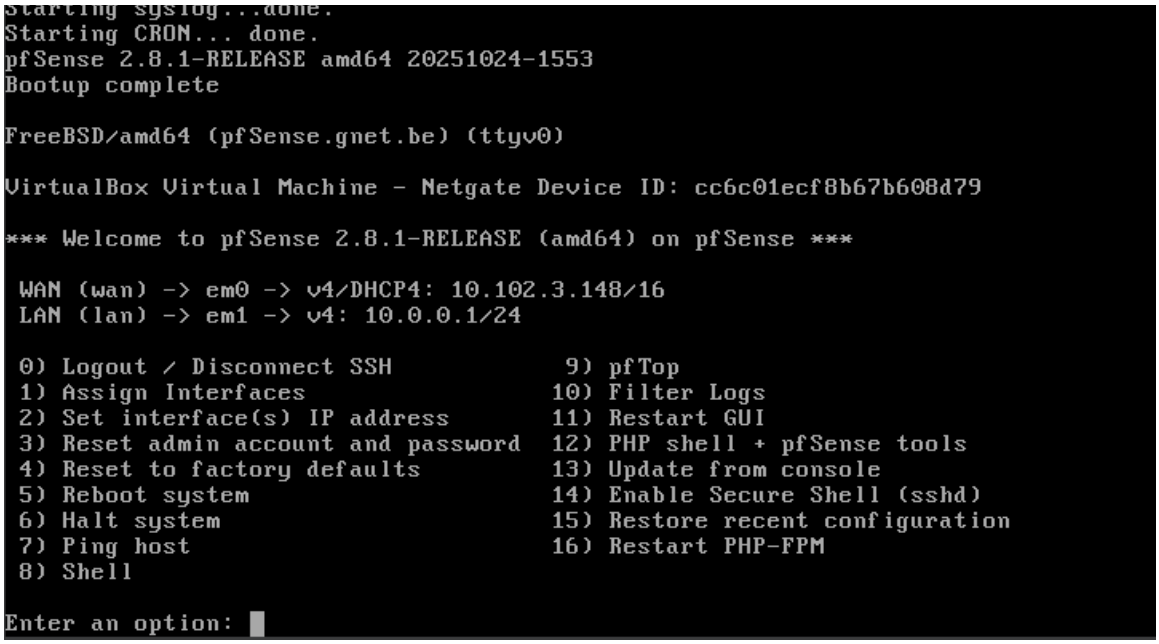
Lors de cette modification, l'accès à l'interface web a été temporairement perdu depuis l'extérieur. Le problème a été résolu en accédant à l'interface de gestion depuis une machine connectée au réseau **LAN**.

2.1 Installation de pfSense

Nous avons installé pfSense à partir de l'ISO officielle.
L'installation s'est déroulée en utilisant les options par défaut :

- Partitionnement automatique,
- Installation de pfSense CE,
- Configuration standard du système.

pfSense a été choisi car il s'agit d'un firewall **open-source**, complet, très utilisé en entreprise et particulièrement adapté à un cadre pédagogique.



2.2 Configuration des interfaces réseau

Deux interfaces réseau ont été configurées dans VirtualBox :

- **WAN** : accès par pont
  Cela permet à pfSense de se connecter directement au réseau physique (réseau de l'école) et donc d'avoir accès à Internet, même si les machines internes utilisent des adresses IP privées.

- **LAN** : réseau interne VirtualBox
  Ce réseau n'existe qu'à l'intérieur de l'environnement virtualisé et permet la communication entre les machines internes (serveur, clients).

Lors de l'assignation des interfaces dans pfSense, une confusion est apparue car les cartes sont nommées *em0, em1*, sans correspondance explicite avec VirtualBox.
Nous avons dû assigner correctement :

- WAN → interface en pont,

- LAN → interface réseau interne.

2.3 Configuration du LAN

Le réseau LAN a été configuré comme suit :

- Adresse IP du firewall (LAN) : **10.0.0.1/24**

- Plage DHCP : **10.0.0.100 → 10.0.0.150**

pfSense assure plusieurs rôles sur le LAN :

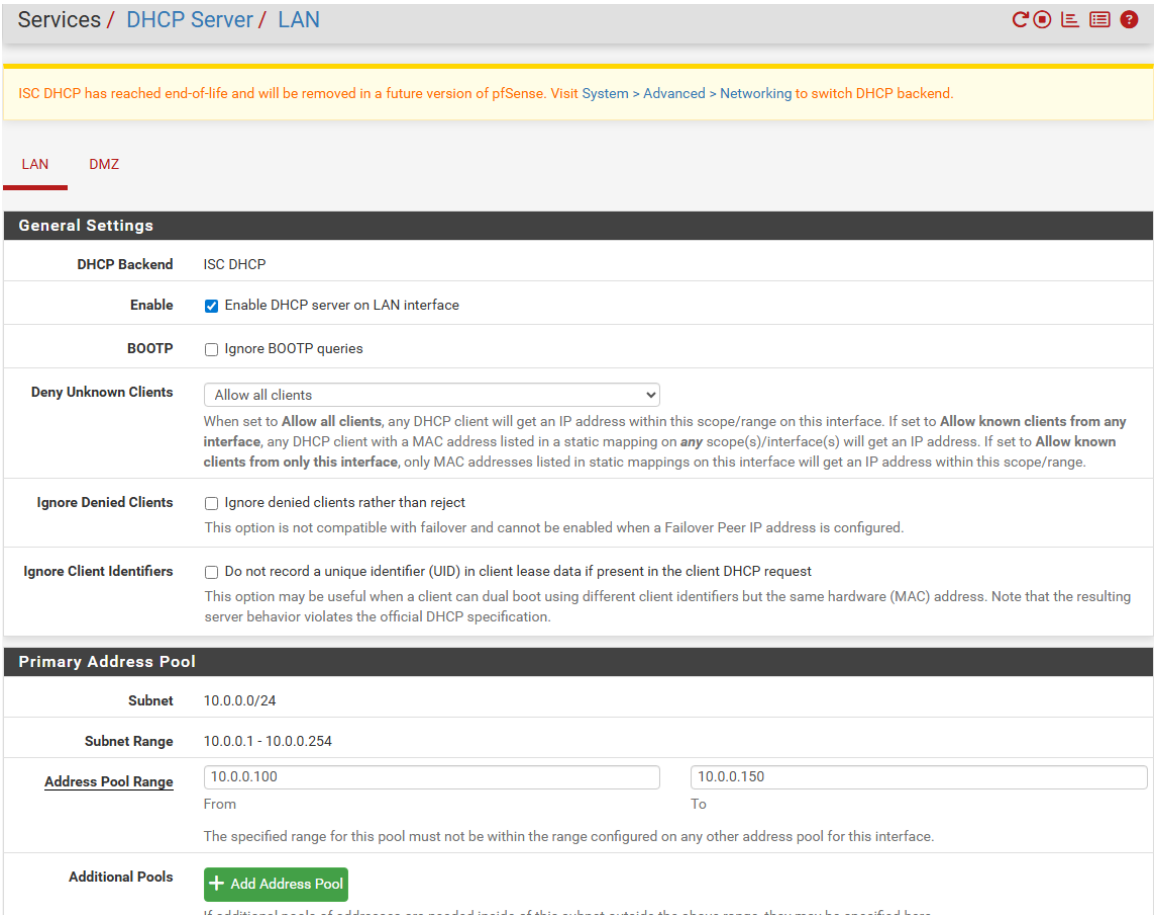
- **Routeur** : passerelle par défaut des machines

- **Serveur DHCP** : attribution automatique des adresses IP

- **DNS** : résolution des noms (resolver / forwarder)

- **NAT** : traduction d'adresses pour l'accès Internet

Grâce au NAT, les machines du LAN peuvent accéder à Internet malgré l'utilisation d'adresses IP privées.



2.4 Accès à l'interface pfSense et problème rencontré

Par défaut, pfSense bloque les connexions provenant du WAN vers son interface d'administration. Ce comportement est normal puisqu'un firewall doit empêcher tout accès extérieur non autorisé.

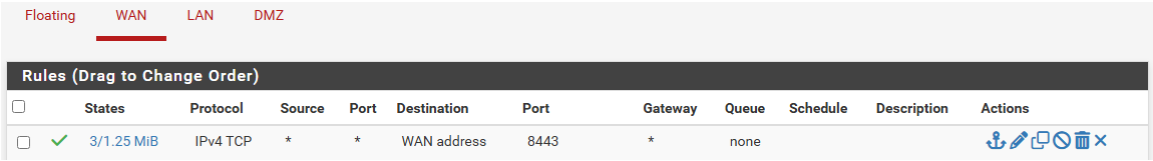
Afin de pouvoir accéder temporairement à l'interface web depuis le WAN, nous avons utilisé la console pfSense pour désactiver momentanément le firewall à l'aide de la commande pfctl -d.

Nous avons ensuite modifié le port HTTPS de l'interface d'administration, en passant du port 443 au port 8443, afin d'éviter un conflit avec d'autres services HTTPS qui seront configurés plus tard dans la DMZ.

Après cette modification, le firewall s'est réactivé automatiquement et l'accès depuis le WAN a de nouveau été bloqué. Comme aucun poste client n'était encore disponible dans le réseau LAN, il n'était plus possible d'accéder à l'interface web de pfSense.

Pour résoudre ce problème, nous avons ajouté une règle sur l'interface WAN du firewall afin d'autoriser les connexions entrantes vers l'adresse WAN de pfSense sur le port 8443. Cette règle permet désormais d'accéder à l'interface graphique du firewall depuis l'extérieur via l'adresse :

http://adresse_wan_du_firewall:8443



Cette règle constitue une exception contrôlée dans la politique de sécurité du firewall, permettant l'administration à distance tout en conservant le blocage du reste du trafic entrant.

3. Installation et configuration de Windows Server 2019

Une machine virtuelle a été créée afin d'installer **Windows Server 2019**.

Après l'installation du système, la configuration réseau a été réalisée manuellement afin d'utiliser une adresse IP fixe.
Cette configuration est nécessaire pour un serveur qui fournit des services réseau.

Les paramètres configurés sont les suivants :

Adresse IP : **10.0.0.99**
Masque de sous-réseau : **255.255.255.0**
Passerelle par défaut : **10.0.0.1** (pfSense)
Serveur DNS : **10.0.0.99**

Le serveur utilise donc **son propre service DNS**, ce qui est nécessaire pour le bon fonctionnement d'un contrôleur de domaine Active Directory.

3.1 Installation du système

Windows Server 2019 a été installé en version **Desktop Experience** afin de disposer de l'interface graphique et des outils d'administration.

L'utilisation d'un serveur dédié permet de centraliser les services réseau et de séparer clairement les rôles.

3.2 Configuration réseau du serveur

Le serveur a été configuré avec une adresse IP stable.

Adresse IP : 10.0.0.99
Masque : /24
Passerelle : 10.0.0.1 (pfSense)
DNS : 8.8.8.8 (serveur DNS de Google pour le moment, puis le serveur lui-même après l'installation d'Active Directory)

Une adresse IP fixe est indispensable pour un contrôleur de domaine, car les clients doivent toujours pouvoir le localiser sur le réseau.

Afin de garantir que le serveur conserve toujours la même adresse IP tout en utilisant DHCP, une **réservation d'adresse IP a également été configurée dans le firewall pfSense**.
Cette réservation associe l'adresse **MAC du serveur Windows** à l'adresse IP **10.0.0.99** dans la configuration du serveur DHCP.

Ainsi, lorsque le serveur demande une adresse IP via DHCP, pfSense lui attribue toujours la même adresse. Cette méthode permet de centraliser la gestion des adresses IP au niveau du firewall tout en conservant une adresse stable pour les services critiques comme Active Directory.

DHCP Static Mappings

IP Address	Hostname	MAC Address	Description	Actions
10.0.0.99	WIN-IRM2021NLUO	08:00:27:a8:ab:70		

3.3 Vérification de l'accès Internet

Une fois la configuration réseau terminée, nous avons vérifié que le serveur pouvait accéder à Internet.

Cette vérification permet de confirmer que :

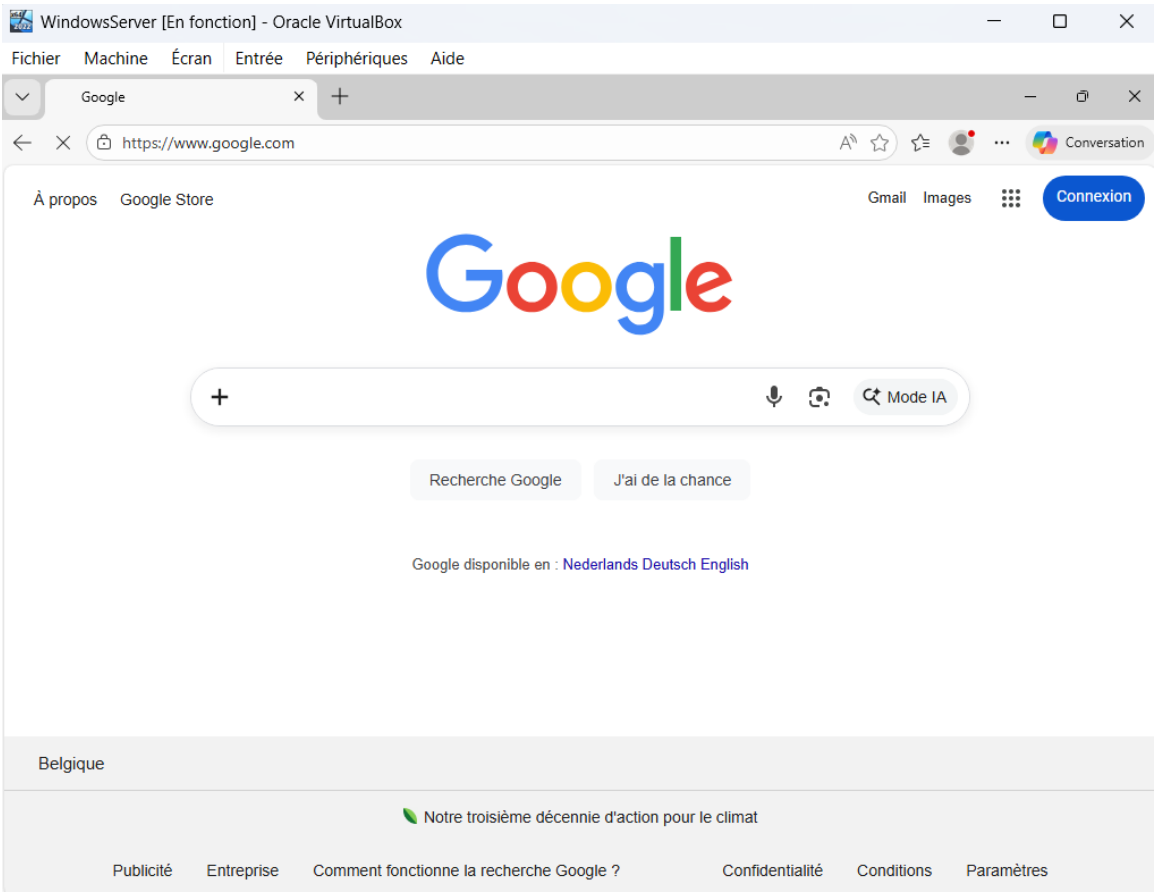
- La passerelle par défaut est correcte
- Le firewall pfSense route correctement le trafic
- Le mécanisme de NAT fonctionne

Le chemin réseau est le suivant :

Serveur → pfSense → NAT → Internet

Un test de connexion a été effectué en utilisant un navigateur web et en tentant d'accéder à un site externe.

L'accès à Internet est rendu possible grâce au **NAT (Network Address Translation)** configuré par défaut sur pfSense. Celui-ci traduit les adresses IP privées du réseau interne vers l'adresse IP publique de l'interface WAN.



4. Mise en place de l'Active Directory

Le rôle **Active Directory Domain Services (AD DS)** a été installé sur le serveur Windows à l'aide du gestionnaire de serveur.

Lors de l'installation de ce rôle, le service **DNS** a également été installé afin de permettre la résolution de noms au sein du domaine.

Le serveur a ensuite été promu en **contrôleur de domaine**, et un nouveau domaine a été créé avec le nom :

gnet.be

Active Directory permet de centraliser la gestion :

- Des **utilisateurs**
- Des **ordinateurs**
- Des **droits d'accès**
- Des **stratégies de sécurité**

Plusieurs comptes utilisateurs ont été créés afin de tester le fonctionnement du domaine, notamment :

- Des **utilisateurs standards**
- Des **administrateurs**

Ces comptes permettent de vérifier les différents niveaux de permissions dans le réseau.

4.1 Installation des rôles AD DS et DNS

Afin de transformer le serveur Windows en **contrôleur de domaine**, il est nécessaire d'installer les rôles **Active Directory Domain Services (AD DS)** et **DNS Server**.

L'installation a été réalisée via le **Server Manager**, qui permet d'ajouter des rôles et fonctionnalités au serveur.

La procédure suivie est la suivante :

1. Ouverture de **Server Manager**
2. Sélection de **Add Roles and Features**
3. Choix de l'option **Role-based or feature-based installation**
4. Sélection du serveur local comme destination

5. Sélection des rôles :
    - **Active Directory Domain Services**
    - **DNS Server**

Lors de la sélection du rôle **AD DS**, Windows propose automatiquement l'installation des **outils d'administration associés**, tels que :

- Active Directory Users and Computers
- Active Directory Administrative Center
- Les outils de gestion PowerShell pour Active Directory

Ces outils permettent d'administrer le domaine, de gérer les utilisateurs et les ordinateurs, ainsi que de configurer les stratégies de groupe.

Le rôle **DNS Server** est également installé, car **Active Directory dépend du DNS pour fonctionner correctement**. Les clients du domaine utilisent le DNS pour localiser les services du contrôleur de domaine et établir les communications nécessaires à l'authentification et à la gestion du domaine.

Une fois ces rôles installés, le serveur peut être **promu en contrôleur de domaine**, ce qui permettra de créer le domaine Active Directory et de centraliser l'administration du réseau.

4.2 Création du domaine

Nous avons créé une nouvelle forêt avec le domaine :

- **gnet.be**

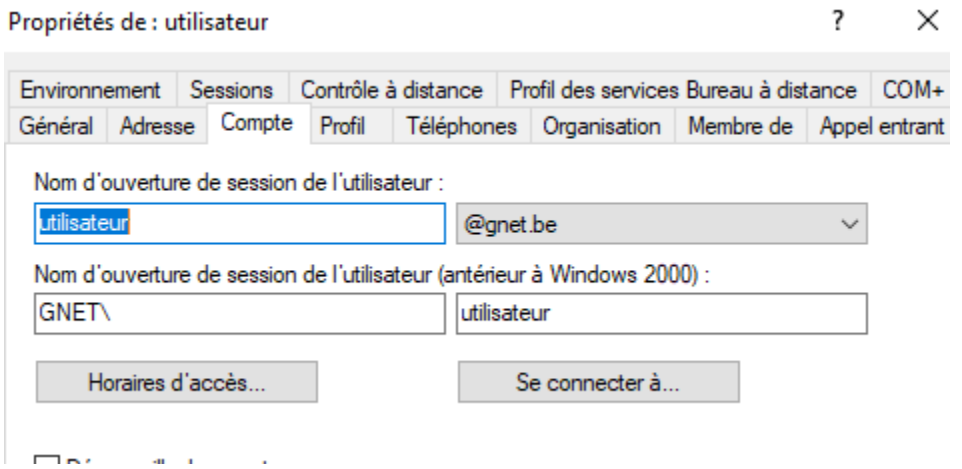
Un mot de passe DSRM a été défini, puis le serveur a redémarré.

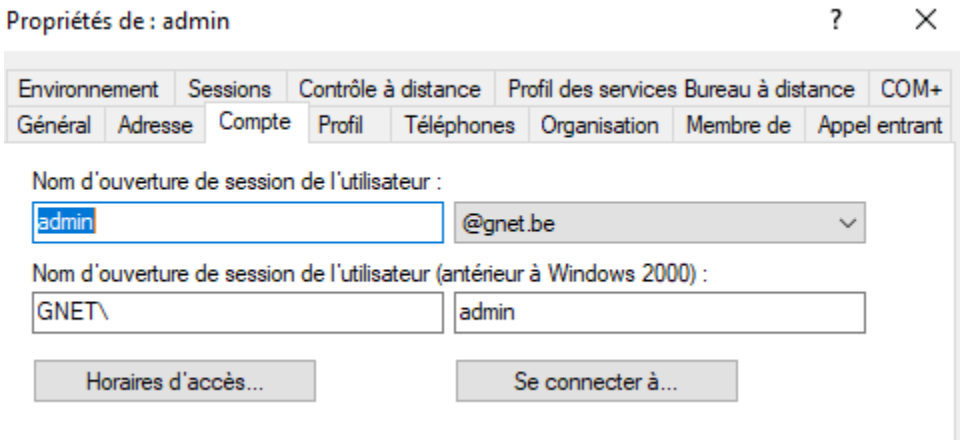
4.3 Création des utilisateurs

Nous avons créé :

- un utilisateur standard,
- un utilisateur avec des droits d'administration.

La séparation des rôles permet de limiter les privilèges et d'améliorer la sécurité.





5. Client Windows (Windows tiny11)

Pour représenter un poste utilisateur du réseau, nous avons installé une machine virtuelle Windows.
La version **Tiny11** a été choisie car elle est plus légère que la version standard de Windows 10 et nécessite moins de ressources, ce qui facilite son utilisation dans un environnement de machines virtuelles.

Le client est connecté au **réseau LAN** afin de pouvoir communiquer avec le serveur Windows et le firewall pfSense.

Les paramètres réseau du client sont obtenus automatiquement via le **serveur DHCP configuré sur pfSense**.
Ce serveur DHCP fournit notamment :

- Une adresse IP dans le réseau LAN
- La passerelle par défaut (pfSense)
- L'adresse du serveur DNS

Dans notre configuration, le serveur DNS fourni aux clients est le **contrôleur de domaine Active Directory**, ce qui est indispensable pour permettre la jonction au domaine.

5.1 Installation du client

Une machine virtuelle a été créée pour installer le client Windows avec la configuration suivante :

- 20 GB d'espace disque
- 2 GB de mémoire RAM
- Une interface réseau connectée au **réseau interne LAN**

Après le démarrage sur l'image ISO de Windows Tiny11, l'installation a été réalisée en suivant l'assistant d'installation classique de Windows.

Une fois l'installation terminée, la machine est connectée au réseau et reçoit automatiquement sa configuration IP via **DHCP depuis pfSense**.

Cela permet au client d'obtenir :

- Une adresse IP du réseau LAN
- La passerelle par défaut
- L'adresse du serveur DNS

5.2 Configuration DNS du client

Pour qu'un ordinateur puisse rejoindre un domaine Active Directory, il doit impérativement utiliser **le serveur DNS du contrôleur de domaine**.

En effet, Active Directory utilise le DNS pour localiser les services du domaine, notamment les contrôleurs de domaine responsables de l'authentification.

Dans notre configuration, le serveur DHCP de pfSense distribue automatiquement l'adresse du **serveur Windows (contrôleur de domaine)** comme serveur DNS.

Ainsi, lorsque le client tente de rejoindre le domaine **gnet.be**, il peut interroger le serveur DNS du domaine pour localiser les services Active Directory.

Si le client utilisait un autre serveur DNS (par exemple 8.8.8.8), le résultat serait le suivant :

- L'accès à Internet fonctionnerait
- Mais la **jonction au domaine serait impossible**, car le client ne pourrait pas localiser le contrôleur de domaine.

5.3 Jonction au domaine

Une fois la configuration réseau et DNS vérifiée, le client Windows a été **joint au domaine Active Directory gnet.be**.

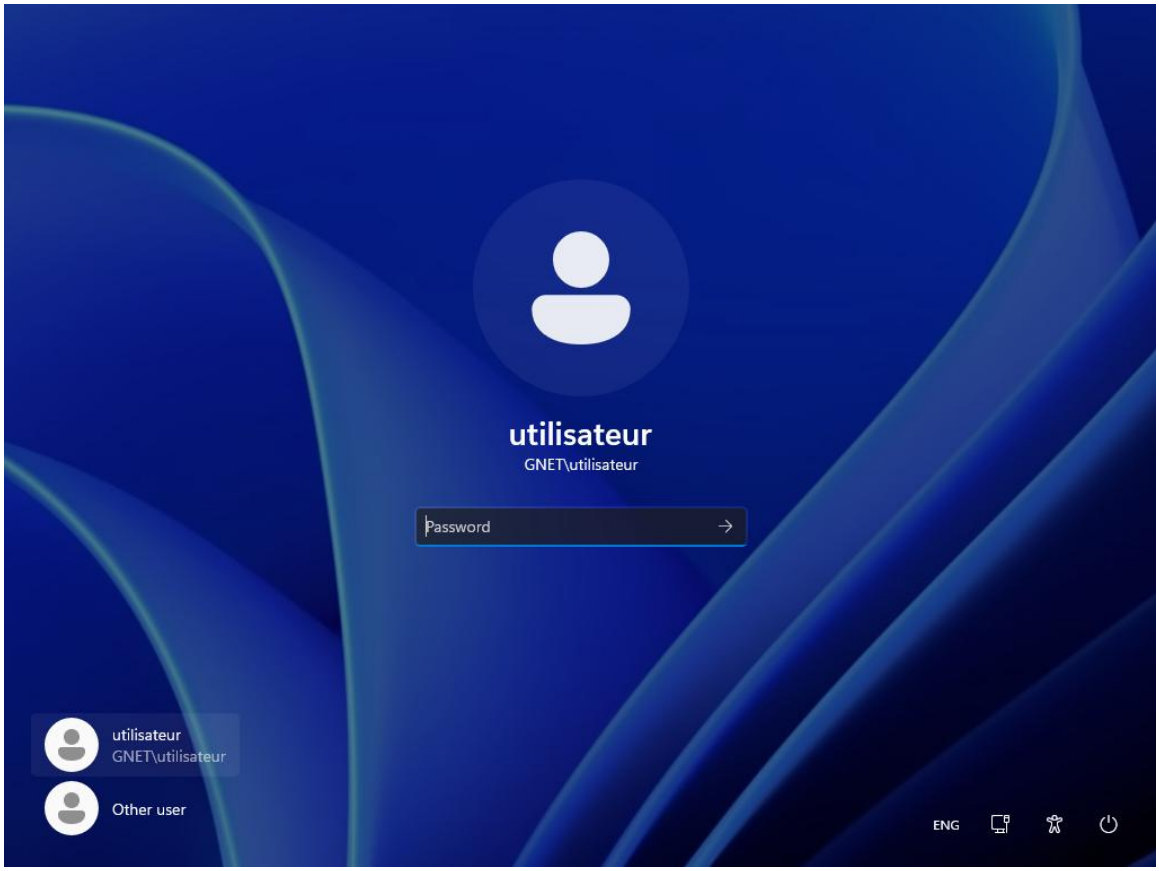
La jonction au domaine a été réalisée depuis les **paramètres système** du client :

1. Ouverture des propriétés système
2. Modification du nom de l'ordinateur
3. Sélection de l'option **Domain**
4. Saisie du nom du domaine : **gnet.be**

Le système demande ensuite les identifiants d'un **utilisateur autorisé à joindre des machines au domaine**, généralement un compte administrateur du domaine.

Après validation, le client est ajouté au domaine et un **redémarrage de la machine** est nécessaire pour finaliser l'opération.

Une fois redémarré, il est possible de se connecter avec un **compte utilisateur du domaine**, ce qui confirme que la jonction au domaine est réussie.



6. Serveur de fichiers

Afin de permettre le partage de ressources au sein du réseau, le serveur Windows a été configuré comme **serveur de fichiers**.
Cette configuration permet aux utilisateurs du domaine d'accéder à des dossiers stockés sur le serveur via le réseau.

Dans le cadre de ce laboratoire, plusieurs dossiers ont été créés sur le serveur afin de tester la gestion des accès entre différents utilisateurs du domaine.

Les partages ont été configurés de manière à contrôler l'accès aux ressources selon les **groupes du domaine**.
Cela permet de limiter l'accès à certaines ressources uniquement aux administrateurs, tandis que d'autres dossiers peuvent être accessibles à l'ensemble des utilisateurs du domaine.

Des tests ont ensuite été réalisés avec différents comptes afin de vérifier :

- L’accès des **administrateurs du domaine**
- L’accès des **utilisateurs du domaine**
- Les restrictions appliquées selon les droits configurés

Ces tests ont permis de confirmer que la gestion des accès aux dossiers partagés fonctionne correctement dans l’environnement du domaine.

6.1 Installation du rôle File Server

Afin de permettre le partage de dossiers sur le réseau, le rôle **File Server** a été installé sur le serveur Windows via **Server Manager**.

La procédure est la suivante :

1. Ouverture de **Server Manager**
2. Sélection de **Add Roles and Features**
3. Choix de l’option **Role-based or feature-based installation**
4. Sélection du serveur local
5. Activation du rôle **File Server**

Ce rôle permet au serveur de gérer des **dossiers partagés accessibles depuis le réseau** par les utilisateurs autorisés.

Une fois le rôle installé, il devient possible de créer et administrer des partages réseau directement depuis l’interface du serveur.

6.2 Création des partages et permissions

Plusieurs dossiers ont été créés sur le serveur afin de tester le partage de fichiers dans le domaine.

Deux types de dossiers ont été configurés :

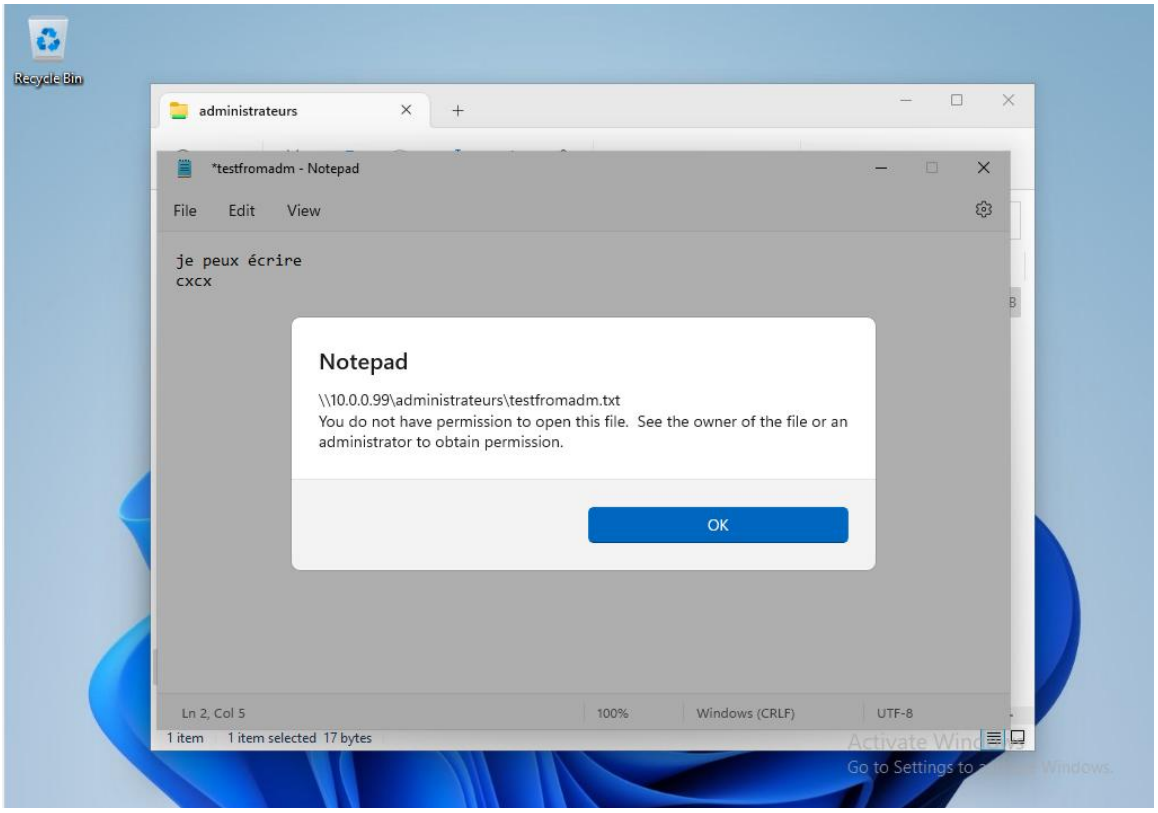
- Un dossier accessible uniquement aux **administrateurs du domaine**
- Un dossier accessible aux **administrateurs** ainsi qu'aux **utilisateurs du domaine**

Ces dossiers ont été configurés comme **partages réseau**, ce qui permet aux utilisateurs d'y accéder depuis les postes clients du domaine.

Depuis un client Windows connecté au domaine, les dossiers partagés peuvent être accessibles via un chemin réseau de type :

\\10.0.0.99

Des tests ont ensuite été réalisés en se connectant avec différents comptes utilisateurs afin de vérifier que les droits d'accès sont correctement appliqués selon le groupe auquel appartient l'utilisateur.

- 

7. DNS et résolution de noms internes

Le DNS interne du réseau est géré par le contrôleur de domaine Active Directory.

Les machines du domaine utilisent ce serveur DNS afin de localiser les services du domaine (contrôleur de domaine, authentication, services réseau).

Pour les requêtes externes vers Internet, un forwarder DNS a été configuré vers pfSense.

Le serveur Active Directory transmet donc les requêtes qu'il ne peut pas résoudre vers pfSense, qui les relaie ensuite vers Internet.

Cette séparation permet :

- au serveur Active Directory de gérer les noms internes
- au firewall pfSense de gérer la résolution externe et l'accès à Internet.

8. IIS – INTRANET

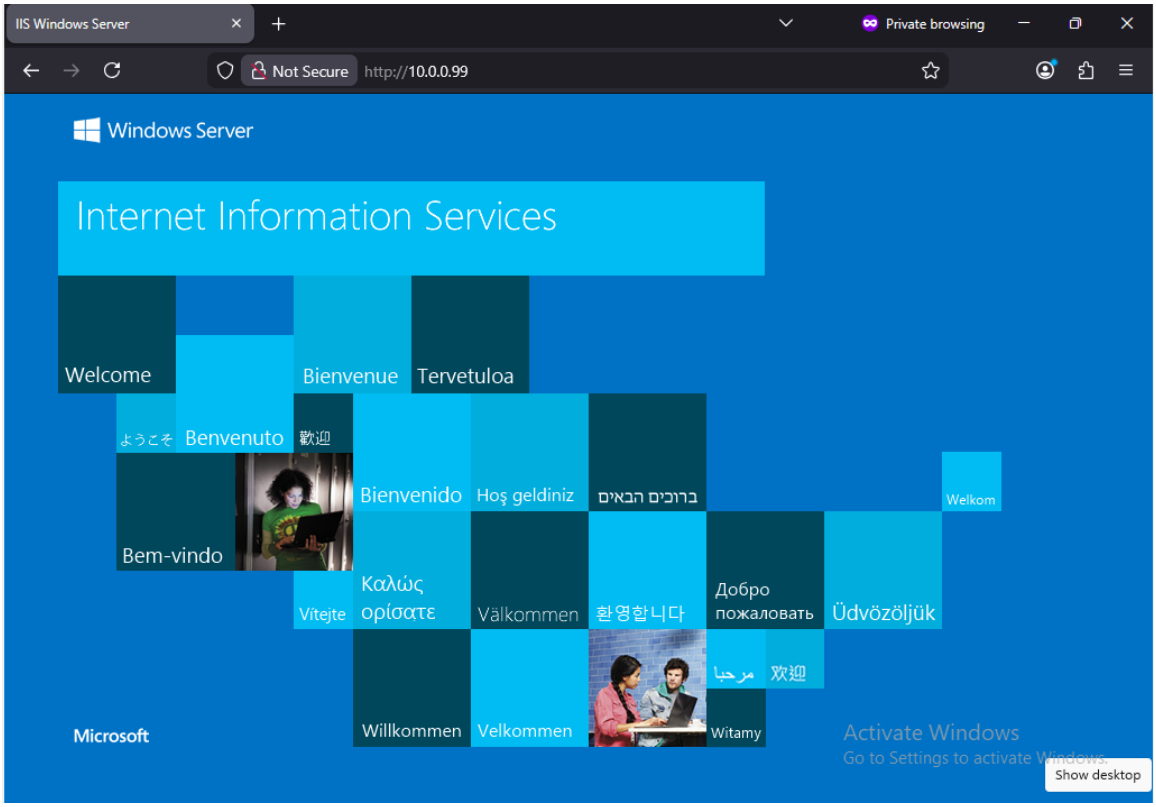
*Afin de mettre en place un **site intranet accessible aux machines du domaine**, le rôle **Internet Information Services (IIS)** a été installé sur le serveur Windows.*

IIS est le serveur web intégré à Windows Server. Il permet d'héberger des sites web accessibles depuis le réseau local ou depuis Internet.

*Dans le cadre de ce laboratoire, IIS a été utilisé pour héberger un **site intranet interne**, accessible uniquement depuis le réseau LAN.*

*Afin de sécuriser l'accès au site, la communication a été configurée en **HTTPS** à l'aide d'un **certificat auto-signé**.*

L'utilisation du protocole HTTPS permet de chiffrer les communications entre le client et le serveur, ce qui garantit la confidentialité et l'intégrité des données échangées.



9. Stratégies de groupe (GPO)

Afin de centraliser l'administration des machines et des utilisateurs, nous avons utilisé les stratégies de groupe (Group Policy Objects).

Deux unités d'organisation (OU) ont été créées dans Active Directory :

• une OU "lab_users" pour les utilisateurs

• une OU "client_pc" pour les machines

Les utilisateurs ont été déplacés dans l'OU "lab_users" et les machines dans l'OU "client_pc".

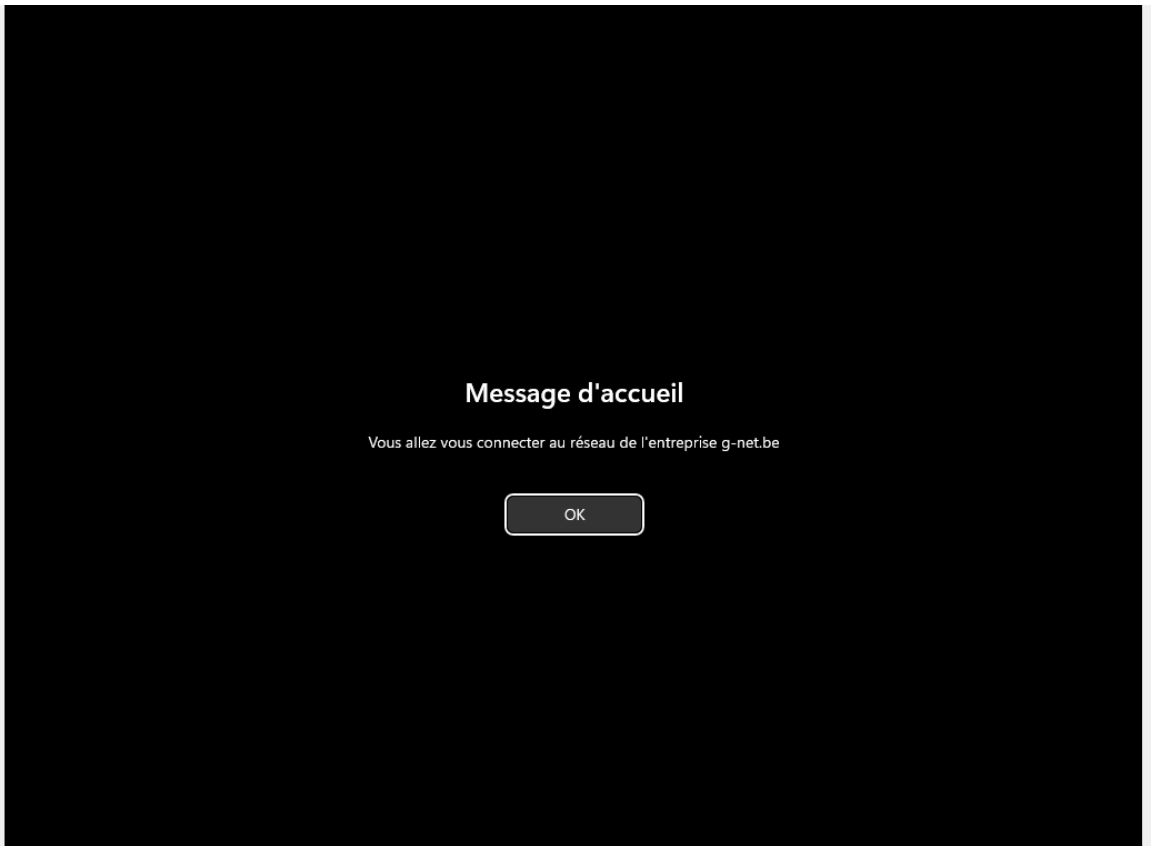
Deux stratégies ont ensuite été configurées :

• Une stratégie appliquée aux machines qui affiche un message d'avertissement lors de la connexion :

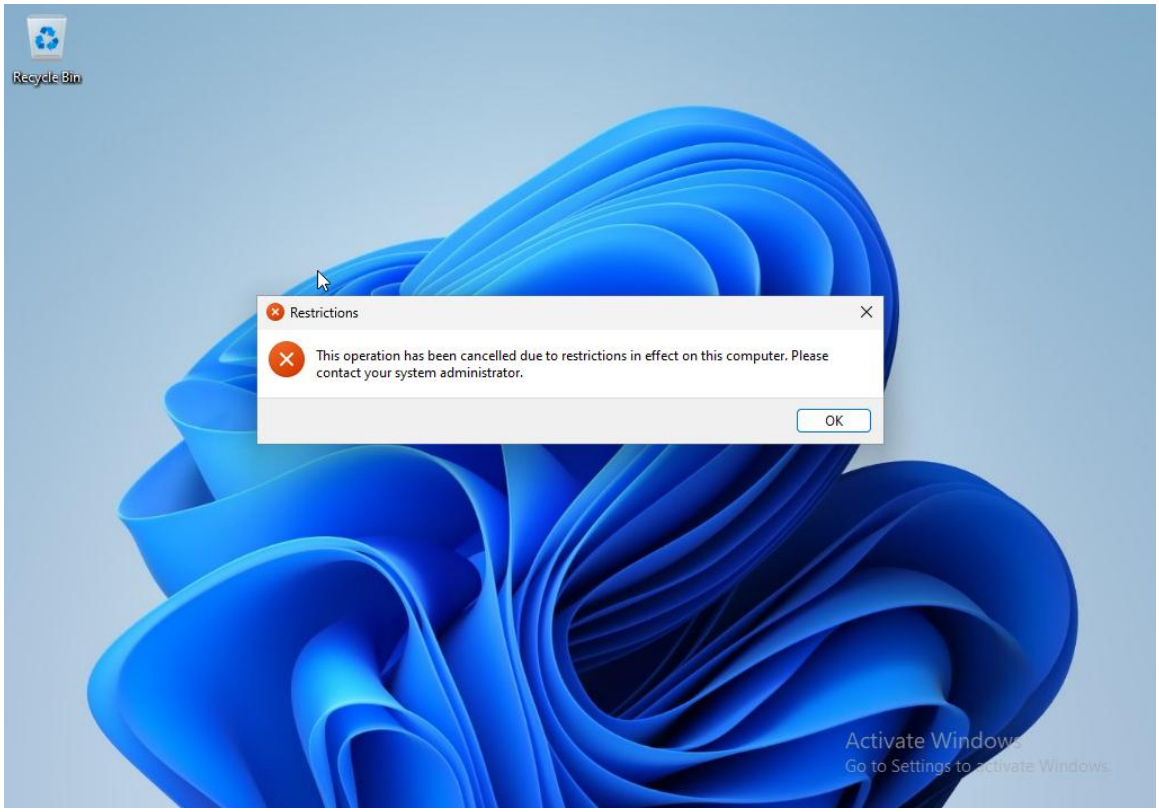
« Vous allez vous connecter au réseau de l'entreprise gnet.be ».

• Une stratégie appliquée aux utilisateurs qui empêche l’accès au panneau de configuration pour l’utilisateur standard.

Les stratégies de groupe permettent d’appliquer des configurations automatiquement à plusieurs machines ou utilisateurs du domaine.



Tentative d'accès au panneau de configuration :



10. PROXY

Un serveur **proxy** a été configuré sur le firewall **pfSense** afin de centraliser et contrôler l'accès web des machines du réseau local.

Ce proxy permet notamment de :

- Centraliser les requêtes HTTP/HTTPS des clients du réseau,
- Améliorer les performances grâce au **cache web**,
- Appliquer des **règles de filtrage** pour limiter l'accès à certains sites.

Dans le cadre du laboratoire, le **cache du proxy a été activé** afin d'optimiser les temps de réponse lors des accès répétés aux mêmes ressources web.

Une **liste noire (blacklist)** simple a également été configurée afin de bloquer l'accès à certains sites web. Des tests ont été réalisés depuis un poste client pour vérifier le bon fonctionnement de cette règle de filtrage.

Les tests ont confirmé que les sites présents dans la blacklist sont correctement bloqués par le proxy.

CONCLUSION

Ce laboratoire nous a permis de mettre en place une infrastructure réseau d'entreprise complète dans un environnement virtualisé.

Nous avons configuré un firewall pfSense, un serveur Windows avec Active Directory, un service DNS interne, un serveur de fichiers, un intranet via IIS ainsi qu'un serveur mandataire (proxy).

Les clients Windows ont été intégrés au domaine et peuvent accéder aux ressources du réseau, ce qui démontre le bon fonctionnement de l'infrastructure.

Ce laboratoire nous a permis de mieux comprendre le rôle des différents composants d'un réseau d'entreprise et leur interaction.