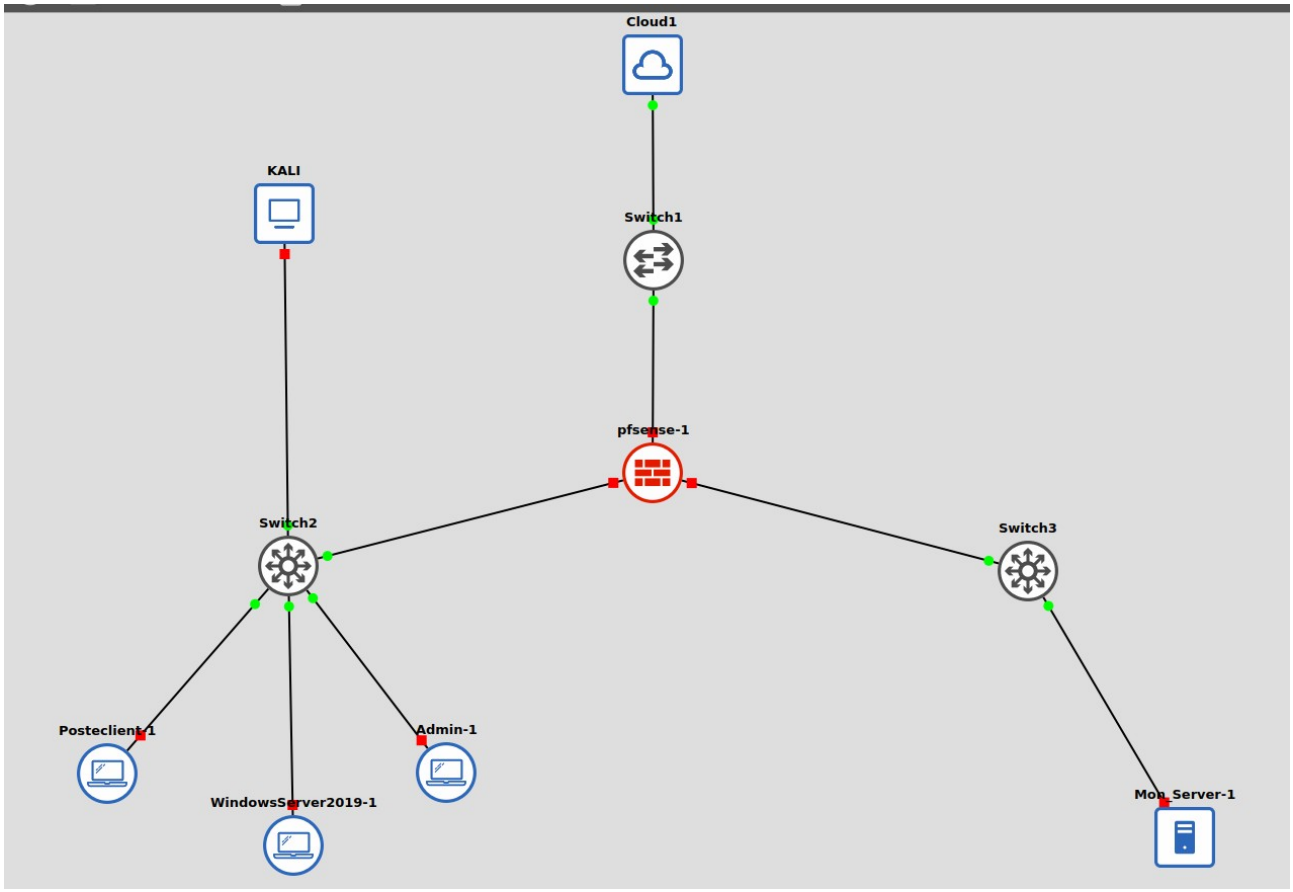
Projet

Titre : Assurer que les données qui circulent dans l’entreprise soient chiffres

Architecture

ZONE	Équipement/OS	Rôle/Fonction	Securite mise en place
WAN	Cloud (accès externe)	Internet	Accès filtrer par pfsense
Pare-feu	Pfsense	Routeur , Pare-feu séparant le WAN , LAN , DMZ	Trafic sécuriser entre le LAN et la DMZ protocoles de securite uniquement (HTTPS , SSH)
LAN	PC Admin	Envoie de fichiers au poste client	Bitlocker , VPN ipsec via Windows serveur
LAN	PC poste client	Réception de fichiers	Bitlocker , Communication IPsec
LAN	Windows server 2019	Serveur VPN et Contrôleur de domaine	GPO IPsec + gestion VPN interne
LAN	KALI LINUX	Machine attaquante	Interception de paquets mais chiffrée
DMZ	Ubuntu serveur	Serveur web (banque) + Base de données	Site Apache2 avec vulnérabilité SQL DB chiffrée



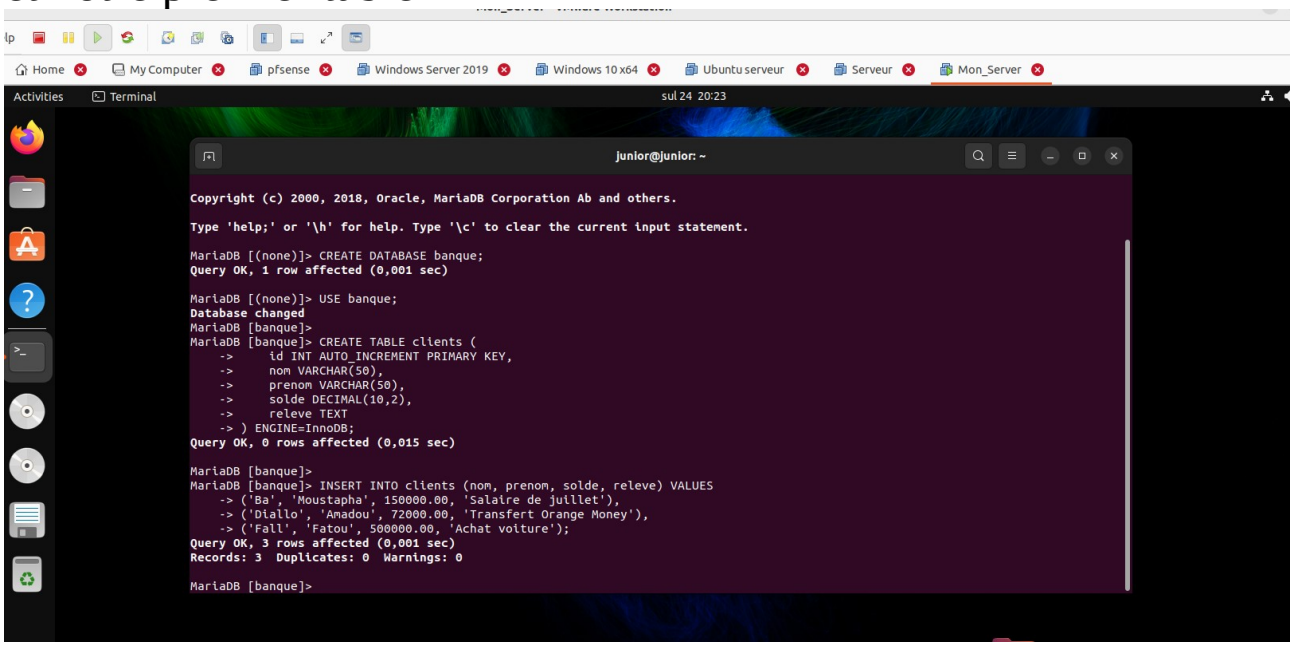
I. <u>Configuration des adresses IP</u>

- Pfsense :
  - Interface LAN => 192.168.100.1/24
  - Interface DMZ => 192.168.200.1/24
  - Interface WAN => DHCP
- Windows Server :
  - Adresse => 192.168.100.10/24
  - Passerelle => 192.168.100.1
- PC Admin :
  - Adresse => 192.168.100.2/24
  - Passerelle => 192.168.100.1
- PC client :
  - Adresse => 192.168.100.3/24
  - Passerelle => 192.168.100.1

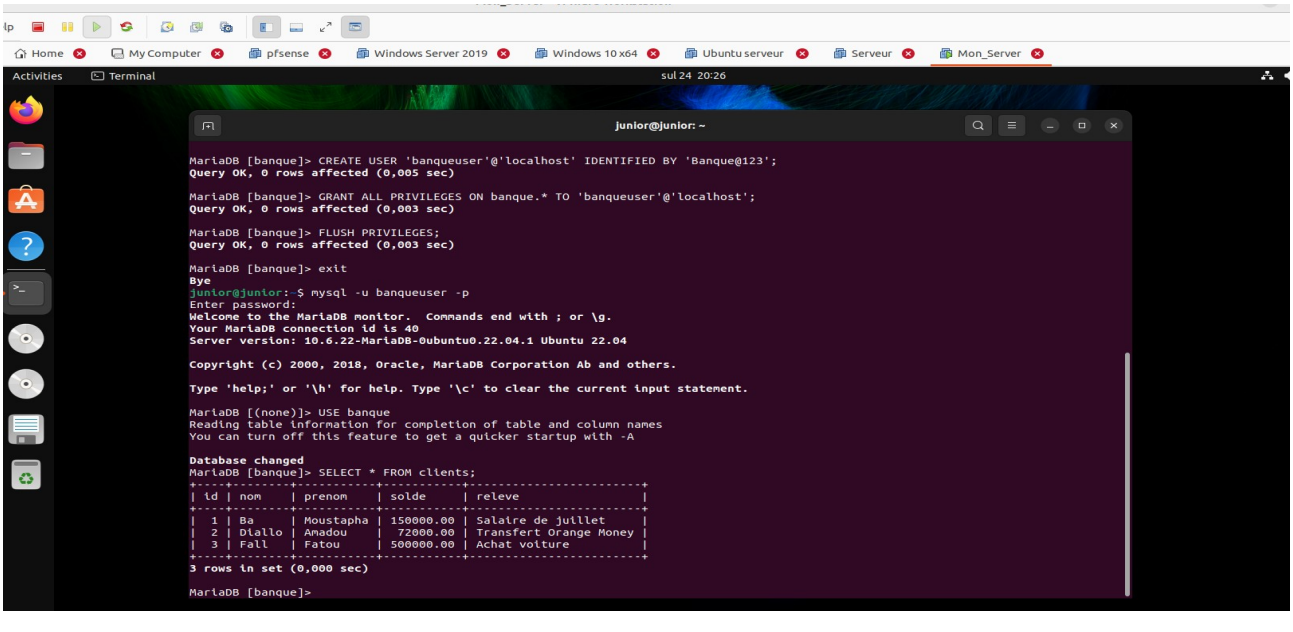
- Kali linux :
    - Adresse => 192.168.100.5/24
    - Passerelle => 192.168.100.1
- Serveur :
    - Adresse => 192.168.200.2/24
    - Passerelle => 192.168.200.1

II. Configuration du Serveur

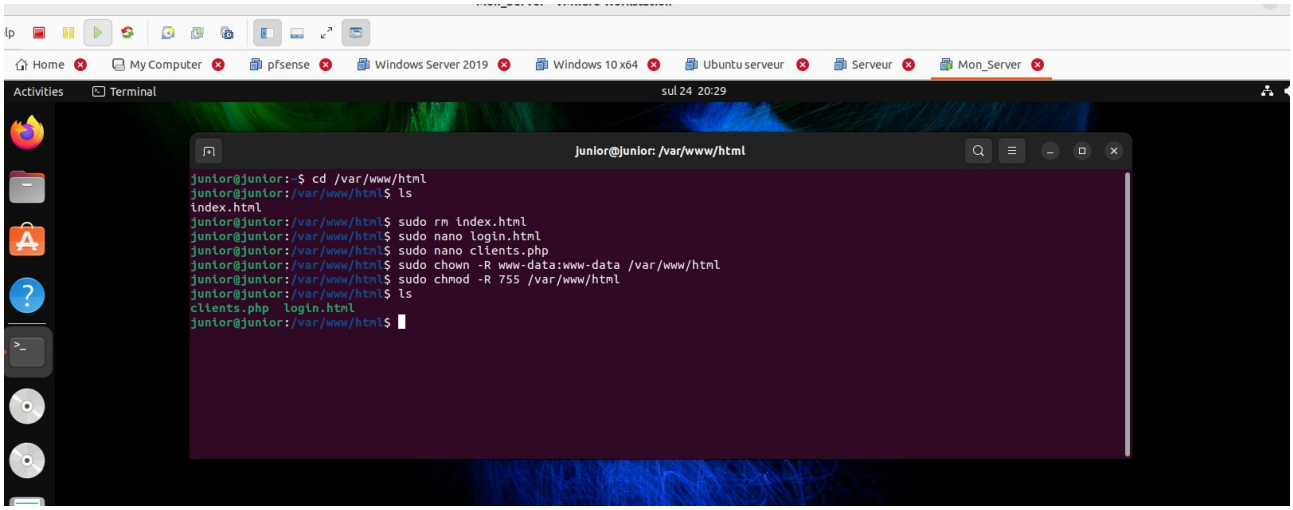
Dans un premier temps on a créer notre base de donnee ‘banque’ , et notre premier table



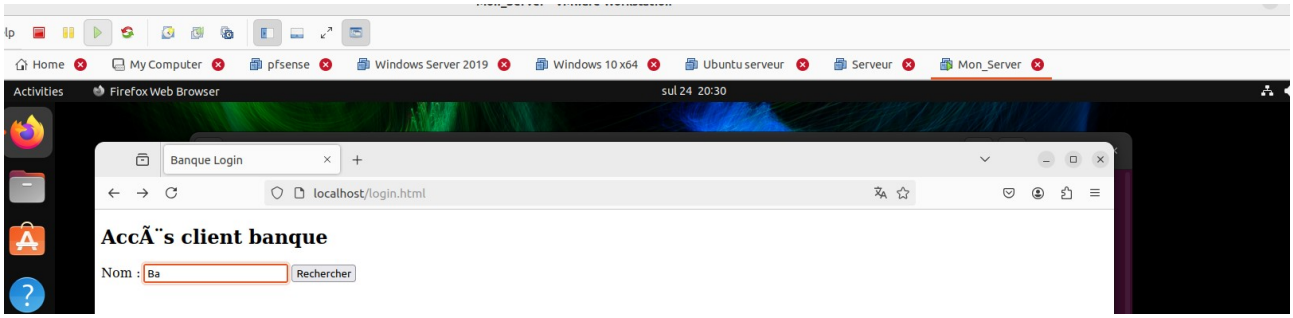
Ensuite , on a créer un utilisateur appele ‘banqueuser’ pour ensuite se connecter avec cette utilisateur

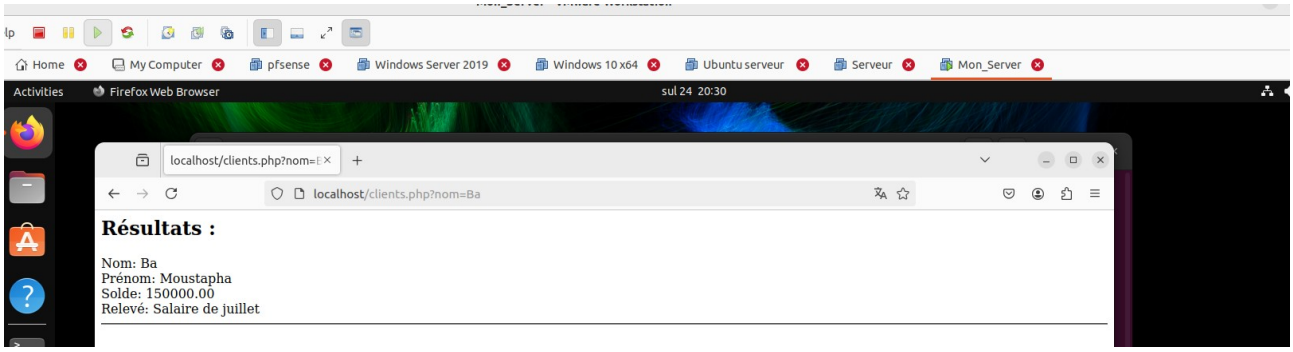


Apres , on a créer nos fichiers (login.html et client.php) et leur attribuer les droits necessaires

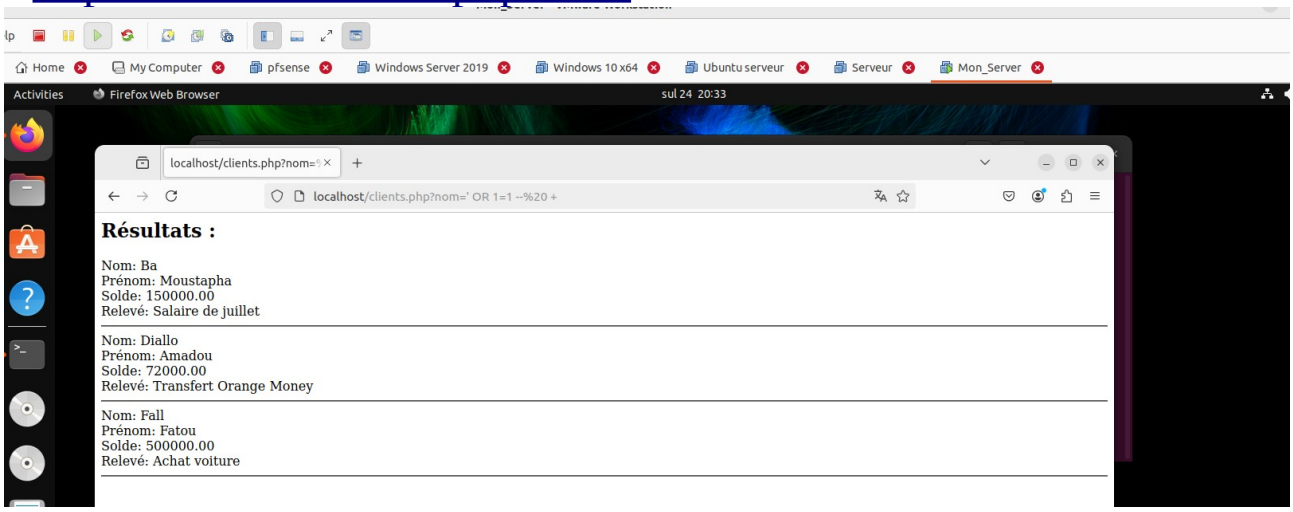


Apres , on est aller dans le navigateur pour verifier si le site fonctionne

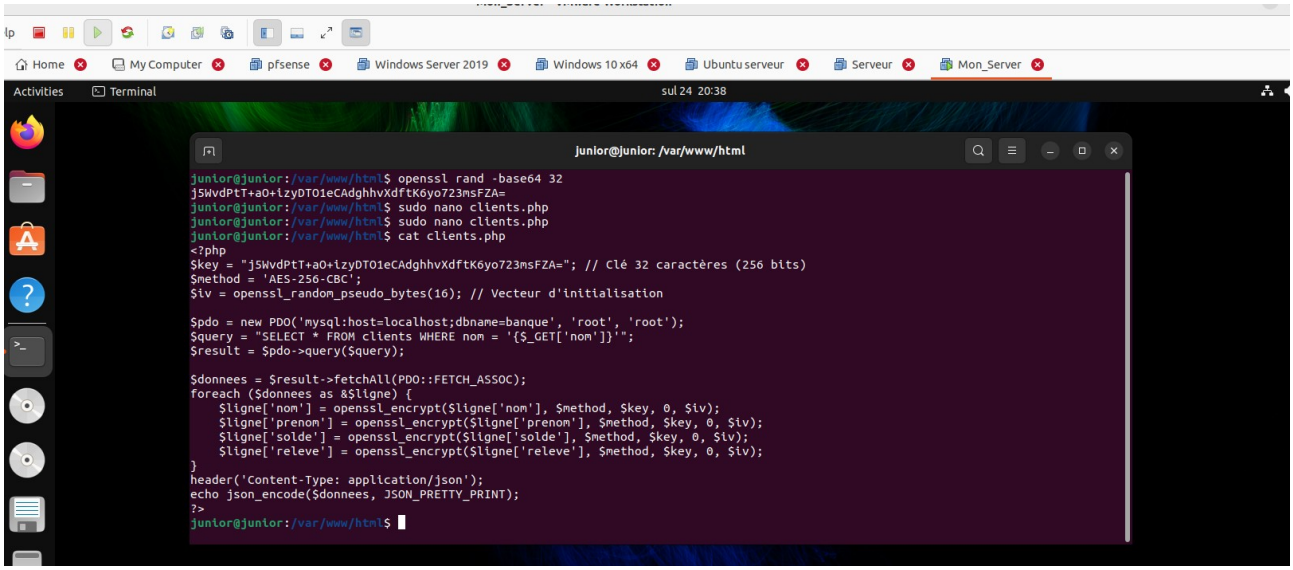




Puis on a tester l’injection sql avec la commande
‘ http://localhost/client.php?nom= ‘ OR 1=1 --

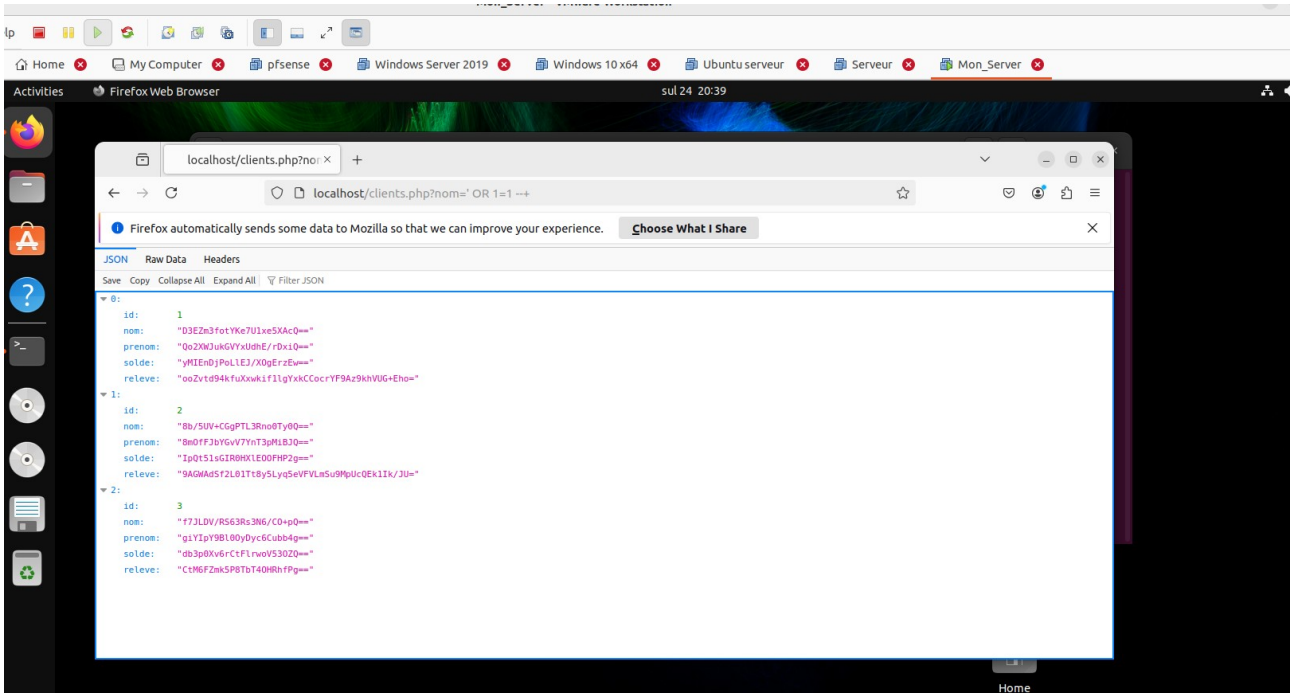


Ici on voit toutes les donnees en claire
Apres cela , on va retourner sur la base pour appliquer le chiffrement



Ici , on a generer dabord une cle de chiffrement puis modifier le fichier client.php pour appliquer le chiffrement

Maintenant on va retourner sur le site et faire le teste d’injection sql a nouveau

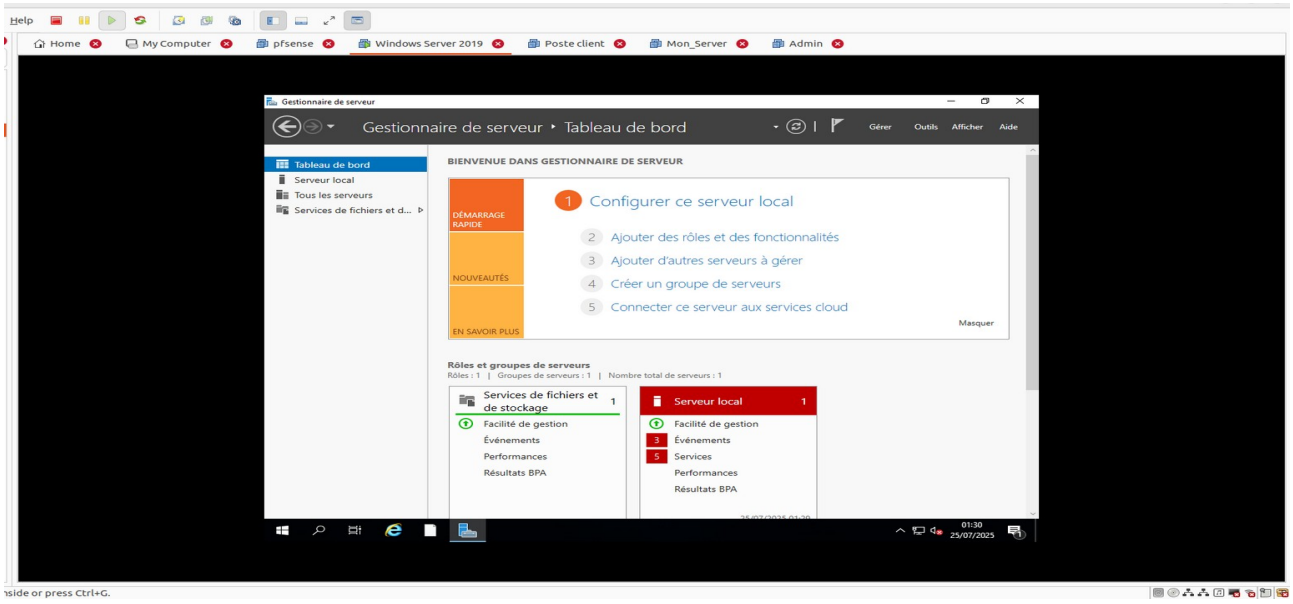


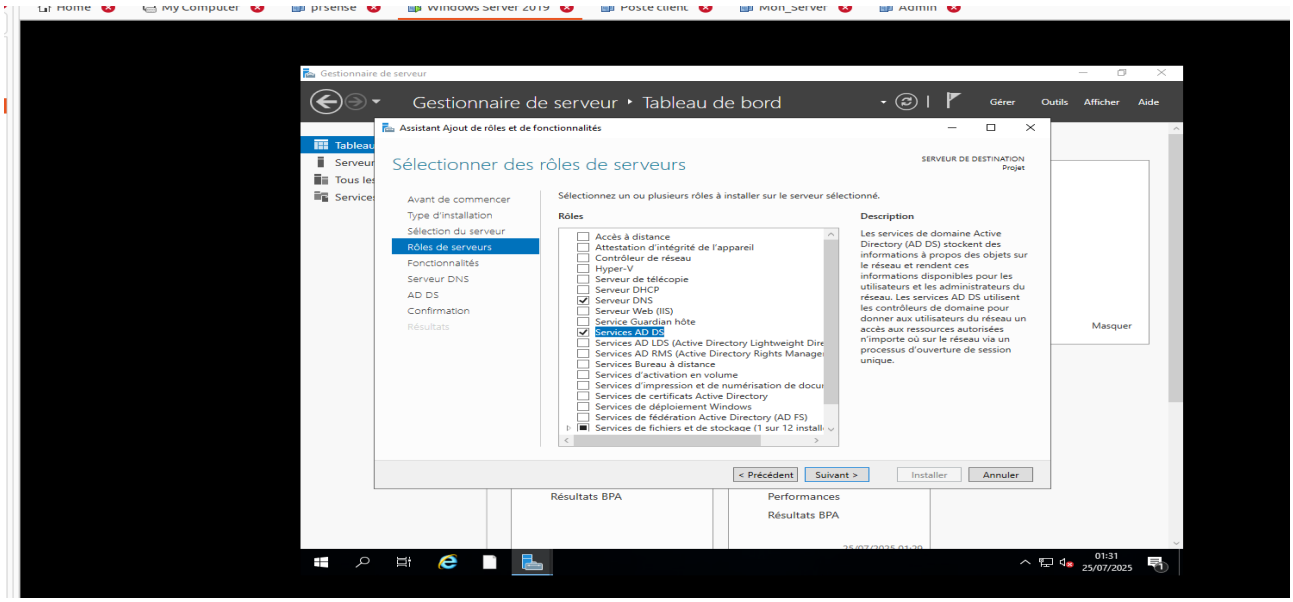
Maintenant , ici on peut conclure que meme si il ya une faille de securite , les donnees sont illisible et peuvent etre dechiffre que par la cle genere tout a lheure

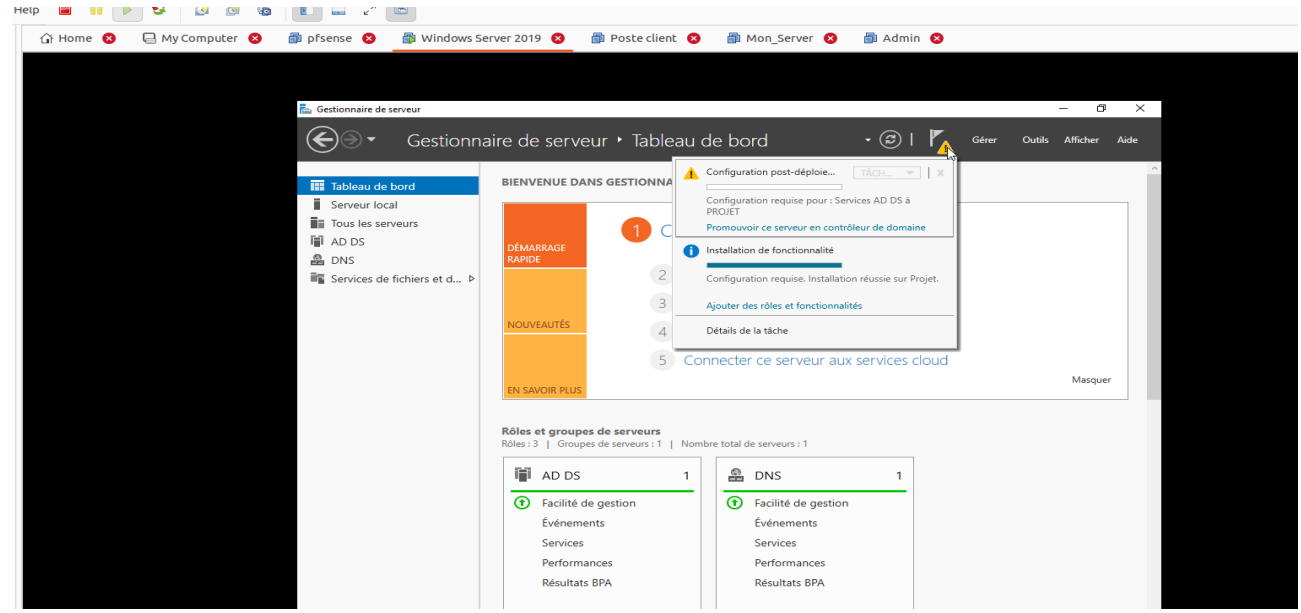
III. Configuration du chiffrement des donnees en transit dans le LAN grace a windows server

Pour cela , on ca créer un controleur de domaine au niveau de windows server , et aller sur les pc concerner pour qu'ils rejoignent le domaine

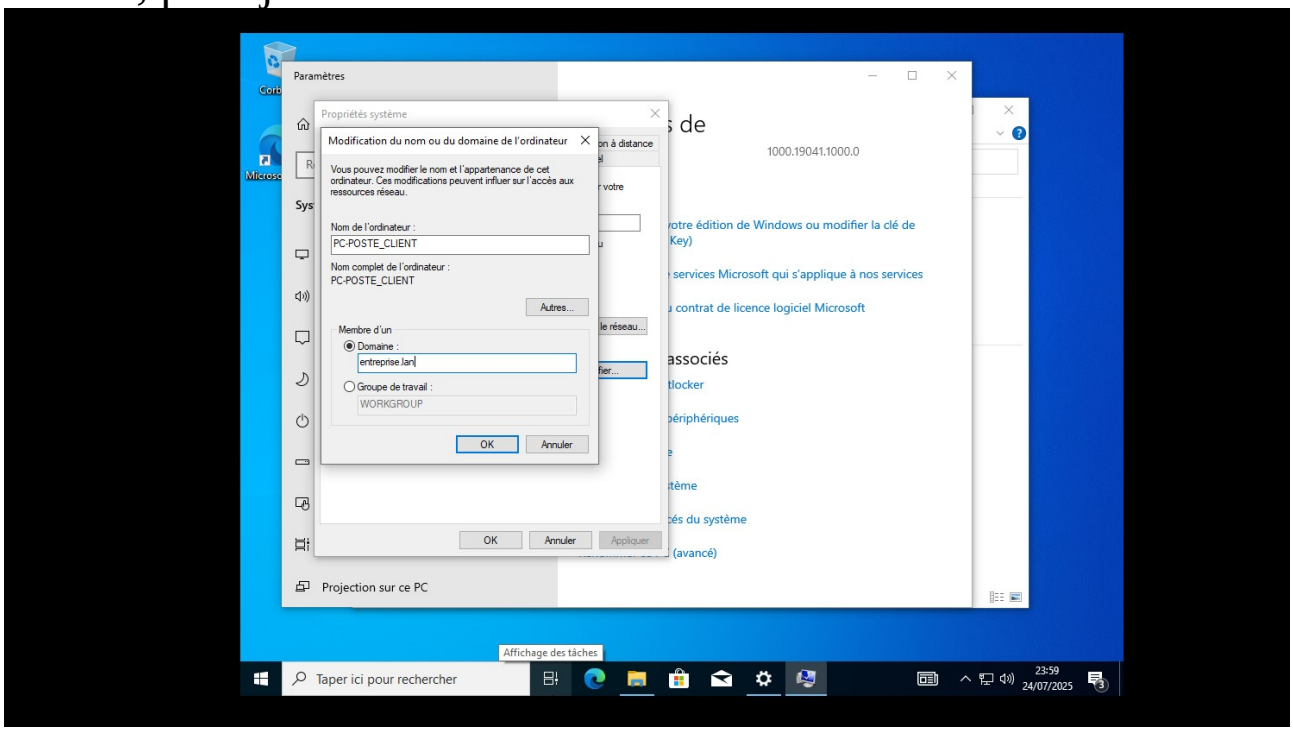
Premierement , on va ajouter des roles au niveau de notre serveur (DNS service et AD DS) puis promouvoir ce serveur en controleur de domaine

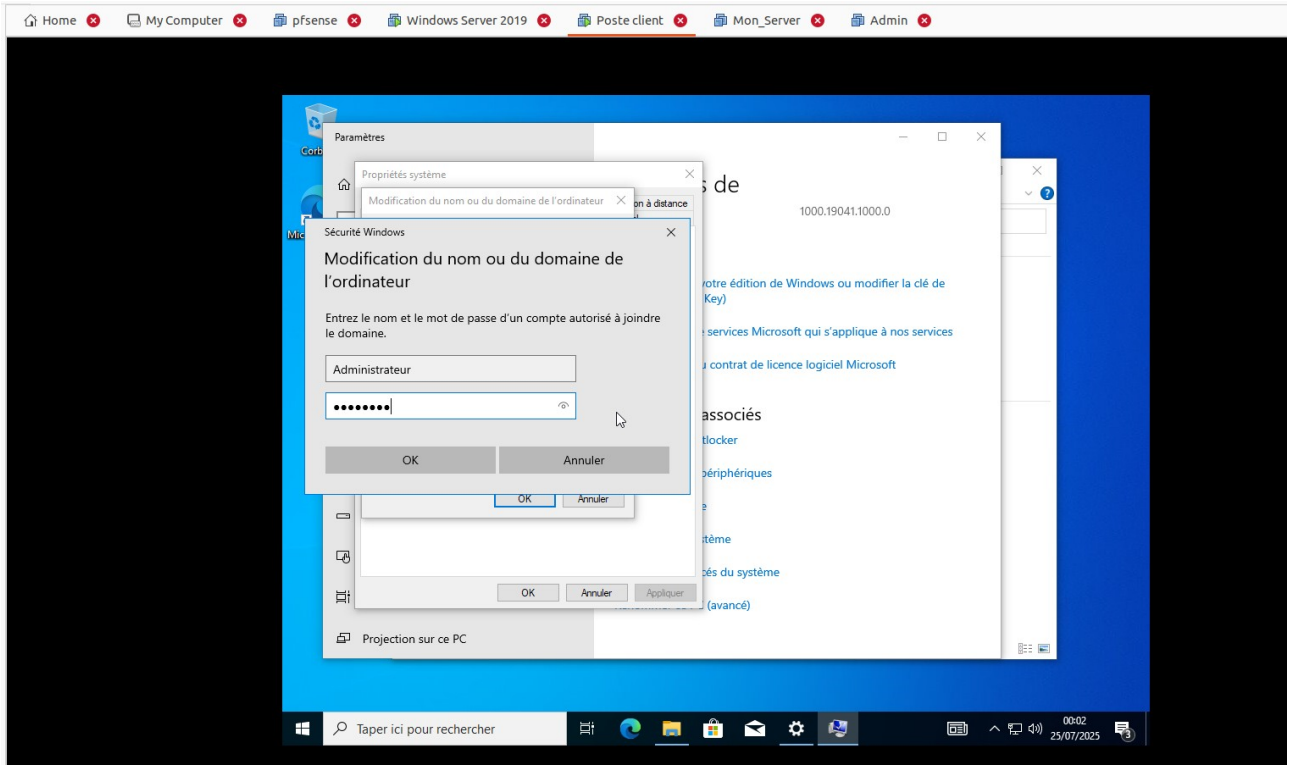

Help
Home
My Computer
pfsense
Windows Server 2019
Poste client
Mon_Server
Admin
Gestionnaire de serveur
Gestionnaire de serveur ▸ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
Services de fichiers et d...
BIENVENUE DANS GESTIONNAIRE DE SERVEUR
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
1 Configurer ce serveur local
2 Ajouter des rôles et des fonctionnalités
3 Ajouter d'autres serveurs à gérer
4 Créer un groupe de serveurs
5 Connecter ce serveur aux services cloud
Masquer
Rôles et groupes de serveurs
Rôles : 1 | Groupes de serveurs : 1 | Nombre total de serveurs : 1
Services de fichiers et de stockage 1
Facilité de gestion
Événements
Performances
Résultats BPA
Serveur local 1
Facilité de gestion
3 Événements
5 Services
Performances
Résultats BPA
01:30
25/07/2025


Gestionnaire de serveur
Gestionnaire de serveur ▸ Tableau de bord
Gérer
Outils
Afficher
Aide
Assistant Ajout de rôles et de fonctionnalités
Sélectionner des rôles de serveurs
SERVEUR DE DESTINATION
Projet
Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DNS
AD DS
Confirmation
Résultats
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.
Rôles
Accès à distance
Attestation d'intégrité de l'appareil
Contrôleur de réseau
Hyper-V
Serveur de télécopie
Serveur DHCP
Serveur DNS
Serveur Web (IIS)
Service Guardian hôte
Services AD DS
Services AD LDS (Active Directory Lightweight Dire
Services AD RMS (Active Directory Rights Manage
Services Bureau à distance
Services d'activation en volume
Services d'impression et de numérisation de docu
Services de certificats Active Directory
Services de déploiement Windows
Services de fédération Active Directory (AD FS)
Services de fichiers et de stockage (1 sur 12 install
Description
Les services de domaine Active Directory (AD DS) stockent des informations à propos des objets sur le réseau et rendent ces informations disponibles pour les utilisateurs et les administrateurs du réseau. Les services AD DS utilisent les contrôleurs de domaine pour donner aux utilisateurs du réseau un accès aux ressources autorisées n'importe où sur le réseau via un processus d'ouverture de session unique.
< Précédent
Suivant >
Installer
Annuler
Masquer
Résultats BPA
Performances
Résultats BPA
01:31
25/07/2025


Help
Home
My Computer
pfsense
Windows Server 2019
Poste client
Mon_Server
Admin
Gestionnaire de serveur
Gestionnaire de serveur ▸ Tableau de bord
Gérer
Outils
Afficher
Aide
Tableau de bord
Serveur local
Tous les serveurs
AD DS
DNS
Services de fichiers et d...
Configuration post-déploie...
Configuration requise pour : Services AD DS à PROJET
Promouvoir ce serveur en contrôleur de domaine
Installation de fonctionnalité
Configuration requise. Installation réussie sur Projet.
Ajouter des rôles et fonctionnalités
Détails de la tâche
DÉMARRAGE RAPIDE
NOUVEAUTÉS
EN SAVOIR PLUS
5 Connecter ce serveur aux services cloud
Masquer
Rôles et groupes de serveurs
Rôles : 3 | Groupes de serveurs : 1 | Nombre total de serveurs : 1
AD DS 1
Facilité de gestion
Événements
Services
Performances
Résultats BPA
DNS 1
Facilité de gestion
Événements
Services
Performances
Résultats BPA

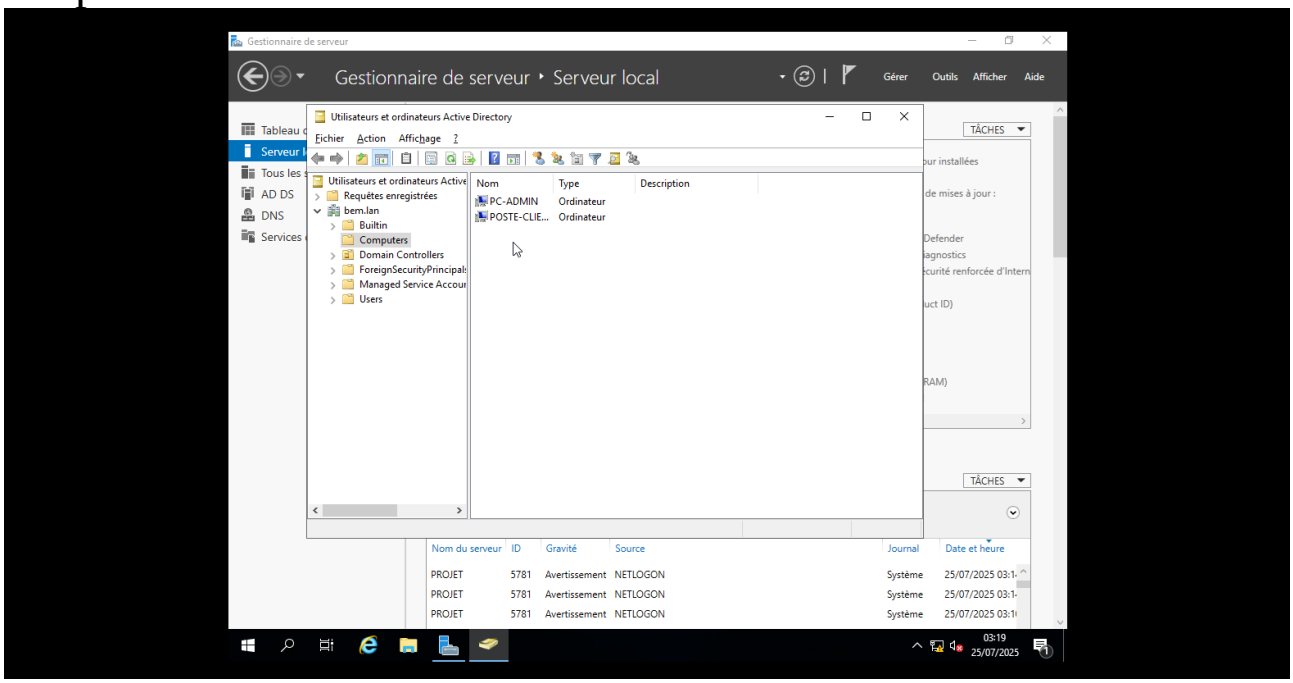
Voilà , notre domaine on l’a nomme entreprise.lan
Maintenant ensuite on va retourner dans nos machines client et admin , pour joindre le domaine



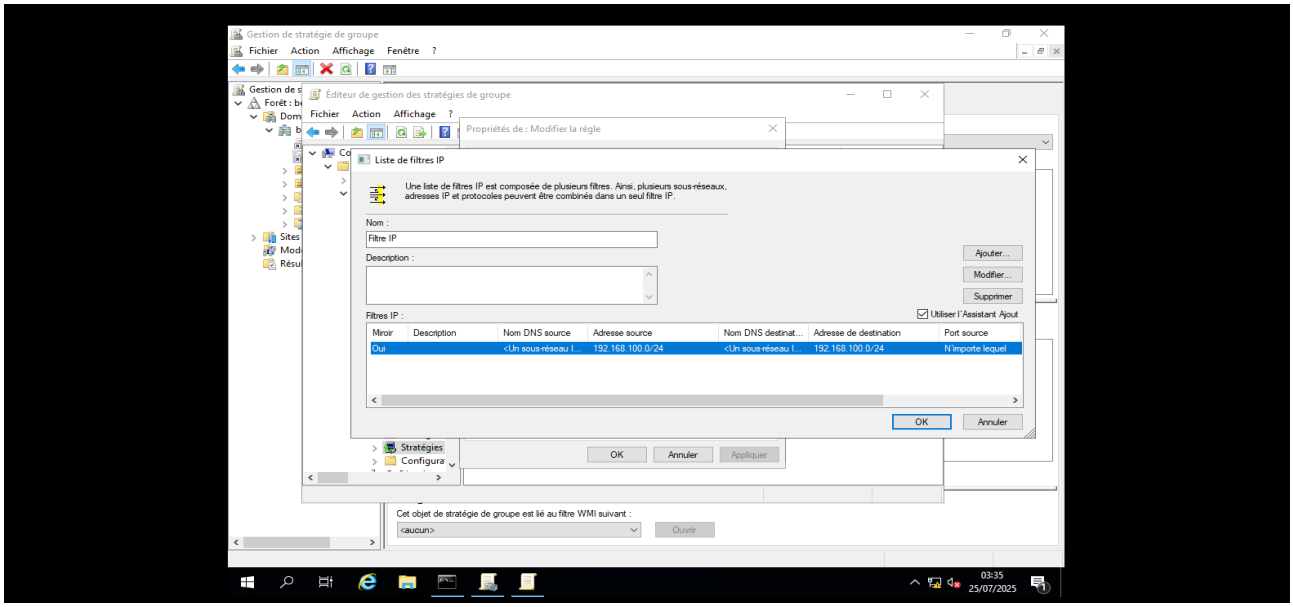


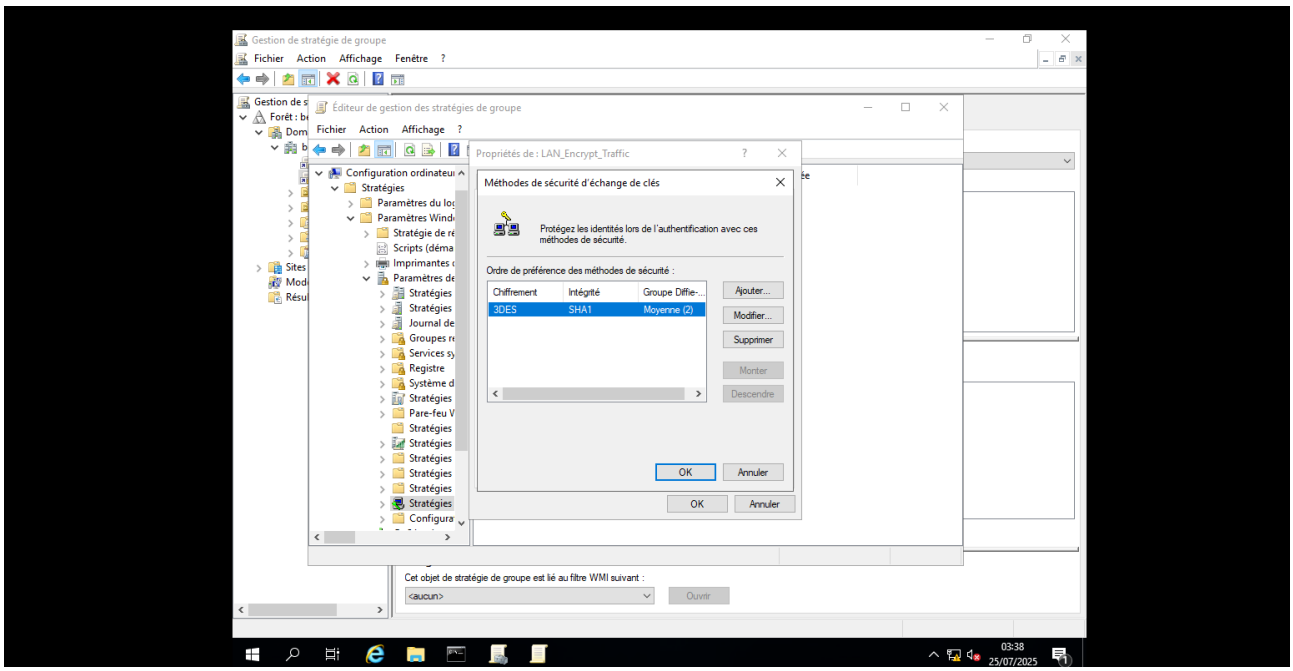
voila , le pc a rejoind le domaine , et on a fait la meme chose pour l’admin

On peut aller verifier au niveau de notre serveur



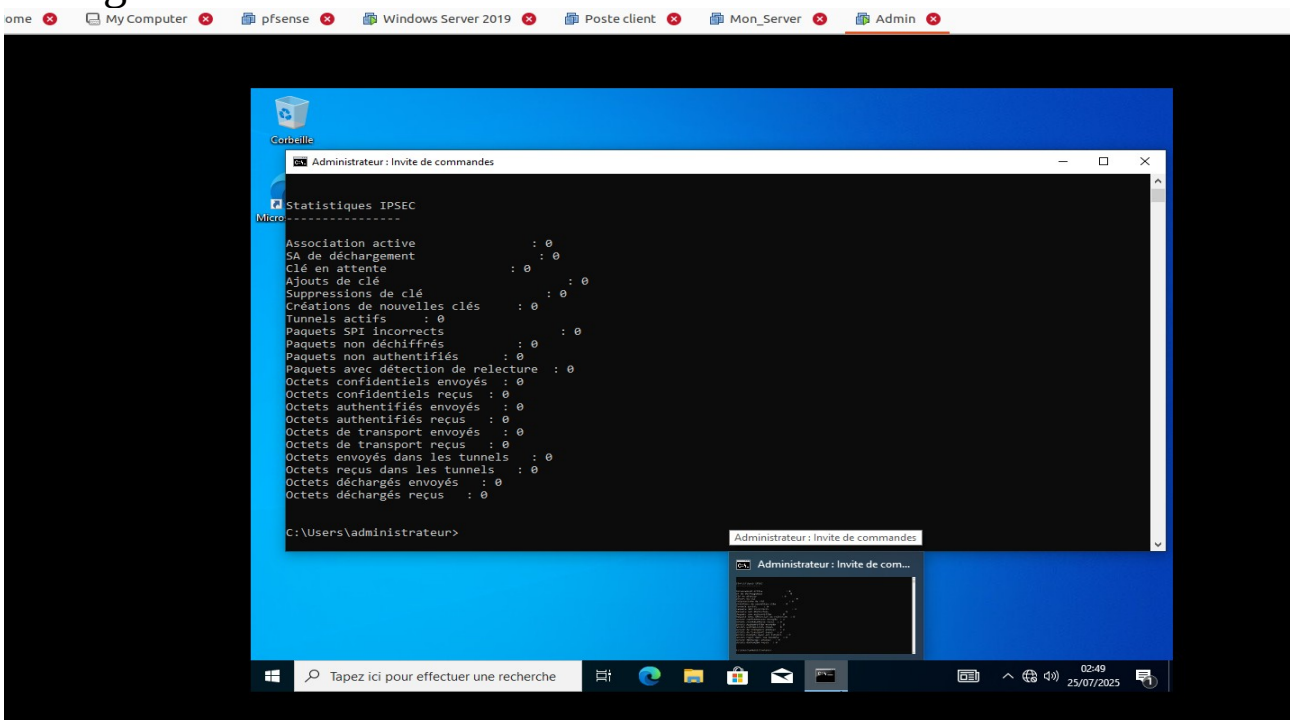
Voilà ici , on voit bien nos deux pc qui rejoingnent le domaine
L’etape suivant consiste a mettre en place une strategie de securite pour faire un filtre Ipsec , au niveau du domaien





Maintenant , ici on a filtrer les echanges sur le reseau 192.168.100.0/24 , puis lier cette strategies de securite au domaine Ceci nous permettra , de definir que meme si la machine KALI a infiltrer le reseau , il n’est pas concerne par le filtrage car il ne fait partie du domaine

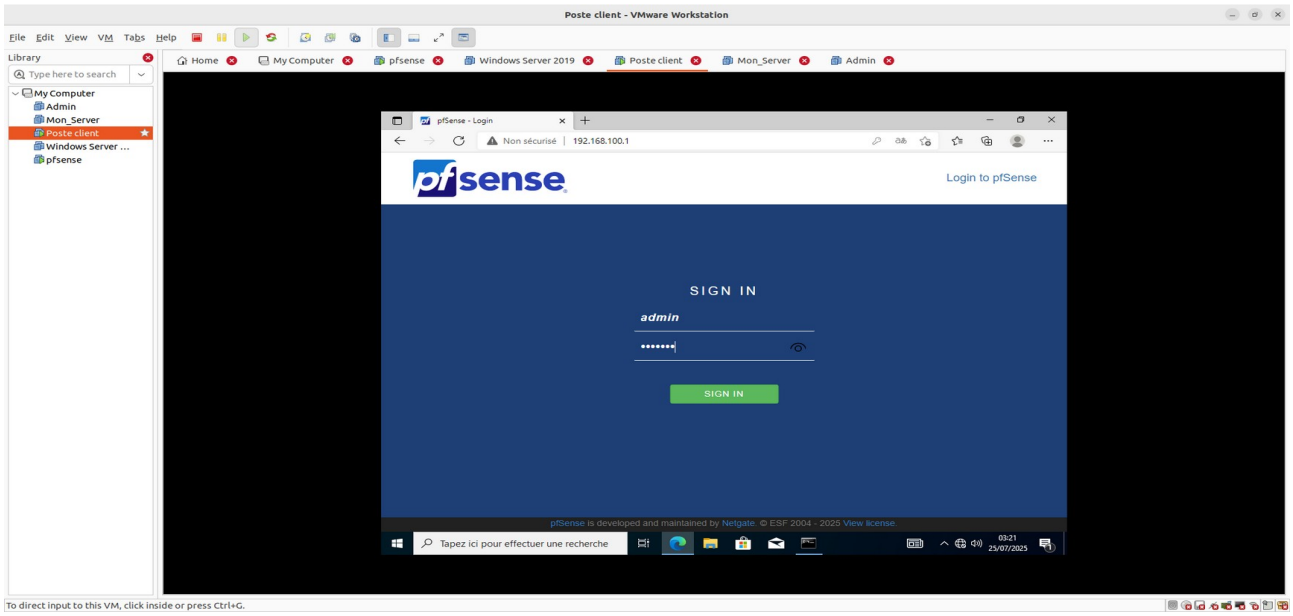
Maintenant , on va verifier au niveau des machines si la configuration d’IPsec a ete mis en succees

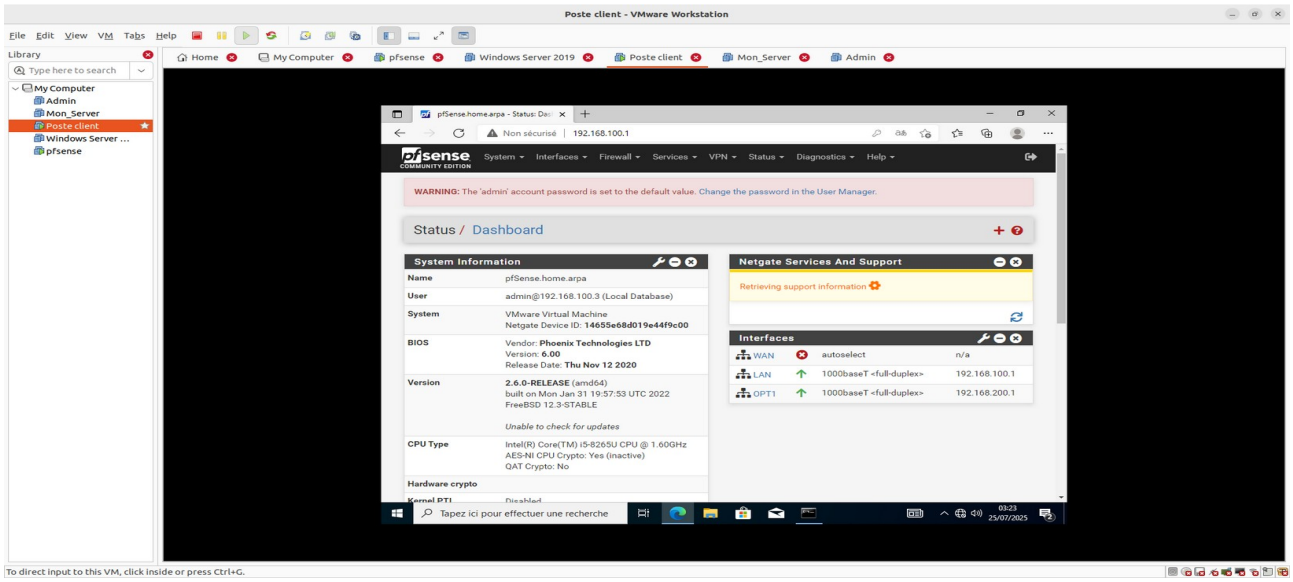


Voilà avec la commande ‘ netsh ipsec dynamic show all ‘ on a peut voir que la configuration est passe avec succes , et on peut meme voir le status
Ici les compteurs sont a zero , car il n’ya pas eu d’echange encore

IV. Configuration de pfsense pour filtrer le trafic

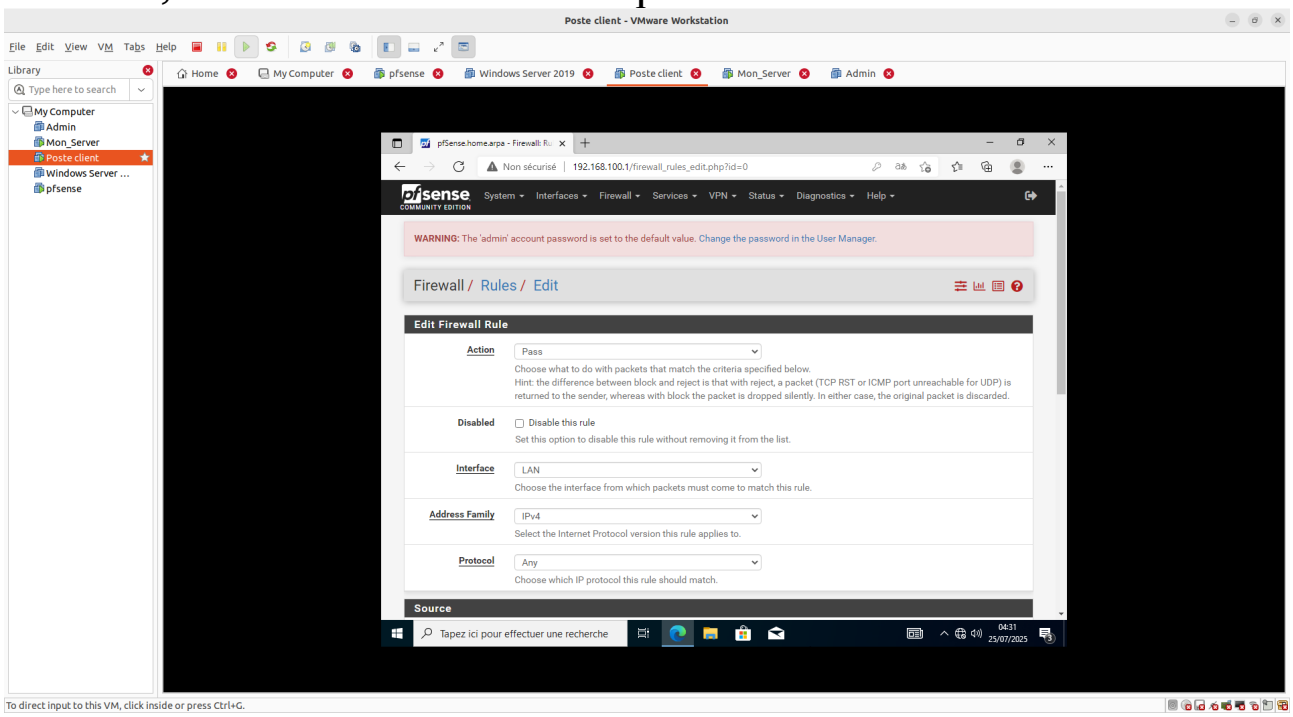
Une fois les configurations faites , cotes LAN et cotes DMZ , avec pfsense , on va autoriser la connexion depuis le LAN vers la DMZ , mais ceci via des protocols de securite comme https , et ssh

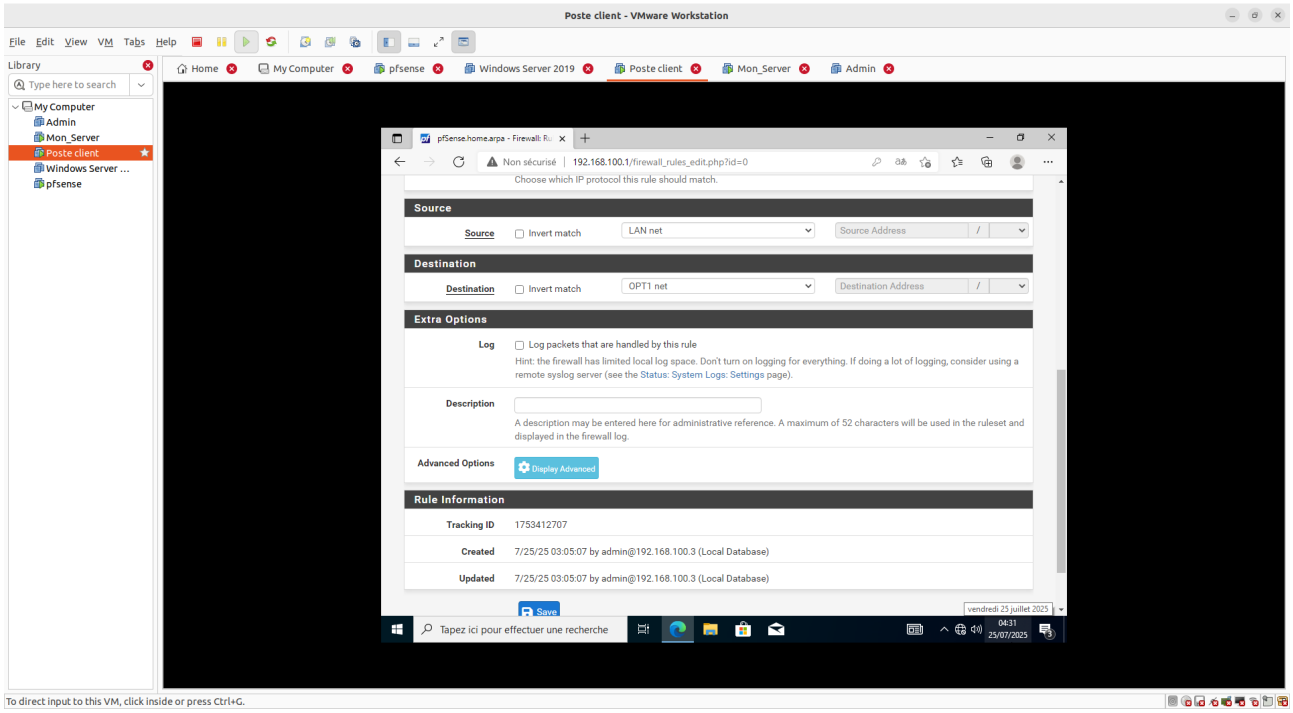


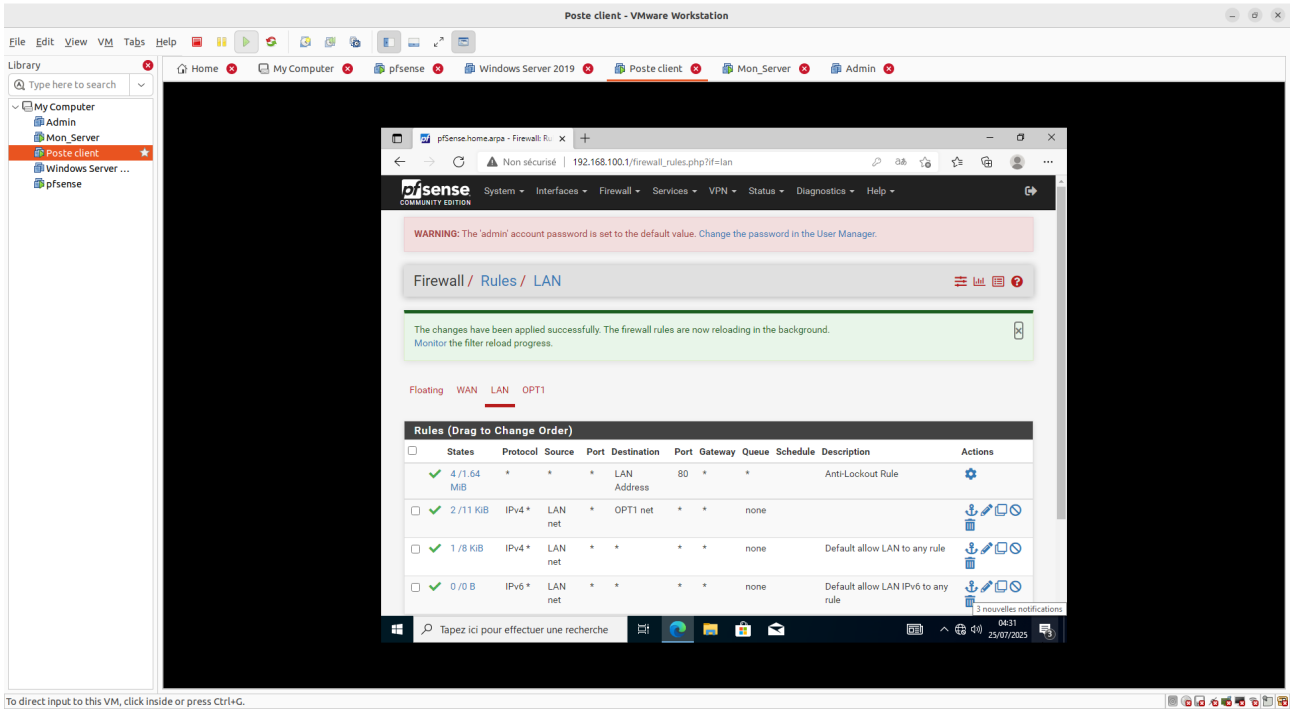


Ici , depuis le LAN on s’est connecter a l’interface graphique de pfsense

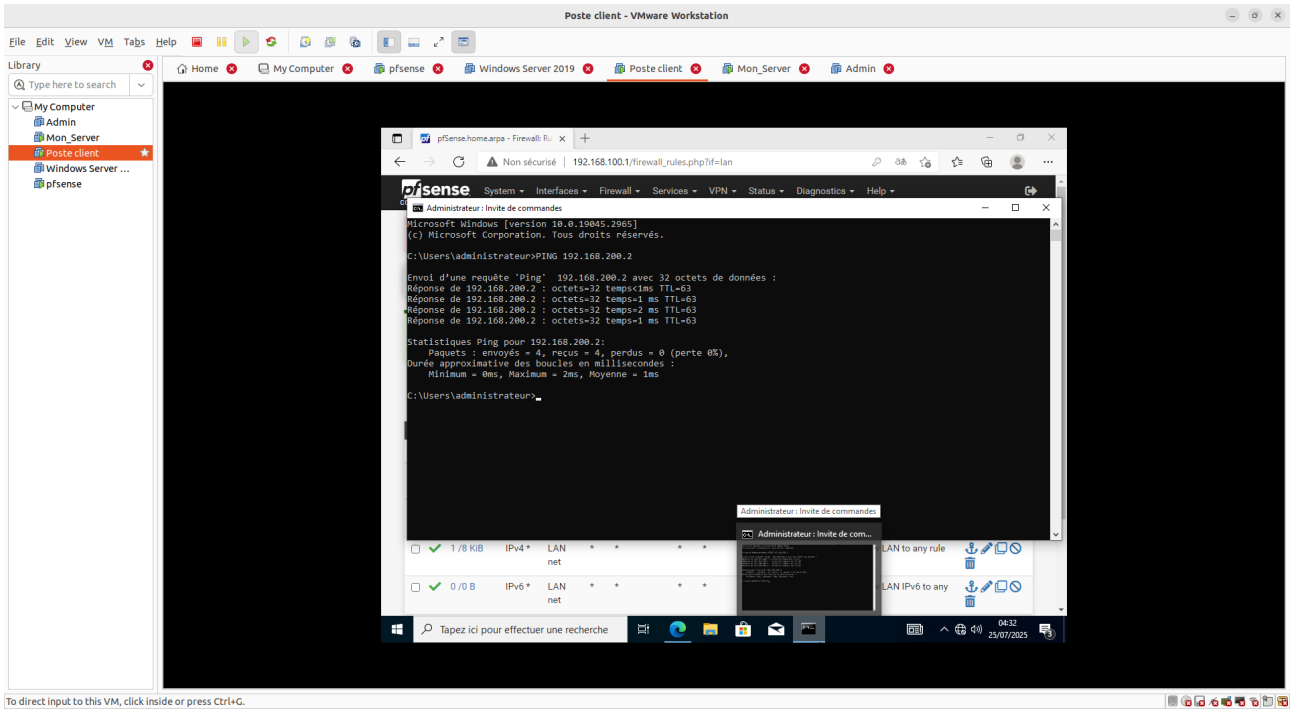
Ensuite , on va definir des roles qui autoriserons le trafic







Une fois ceci fais , on va essayer la connexion , depuis notre pc qui l’adresse 192.168.100.3 vers le serveur 192.168.200.2



Ainsi , notre filtrage nous a permis de faire la connexion , depuis le LAN vers la DMZ

Teste

Depuis la machine kali , on a attaquer la base de donnee , et ceci ne revelle que des donnees chiffre