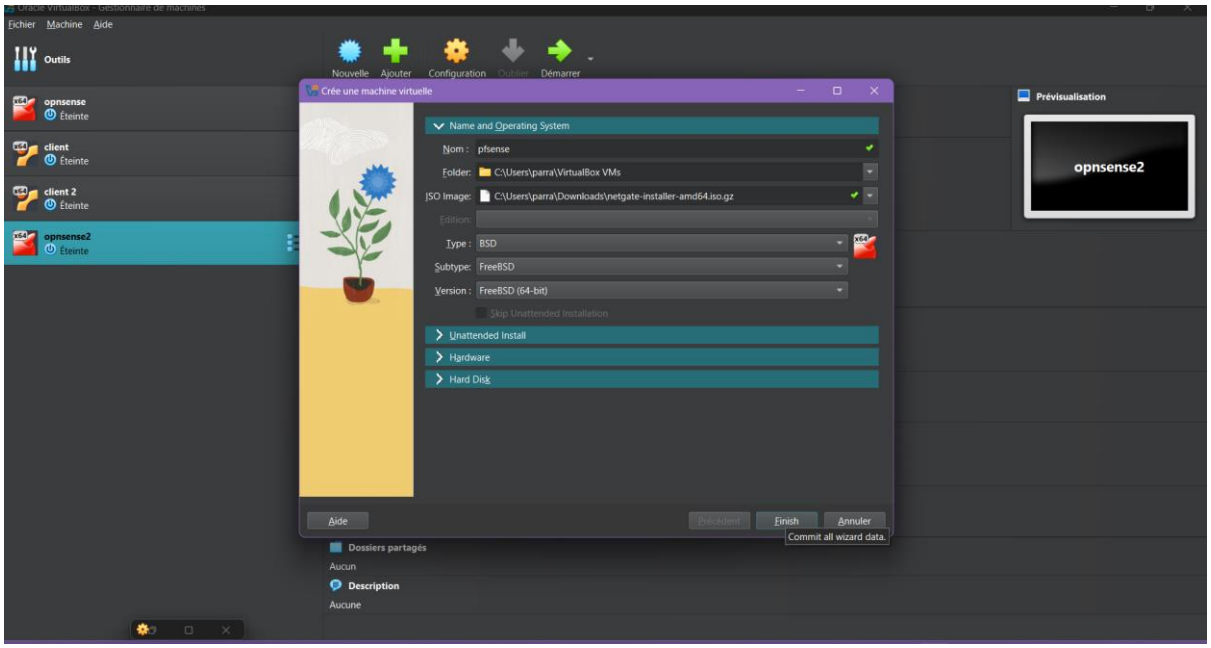
TP : Sécurité avancé à rendre avant le 25/11/2024 fatima ly

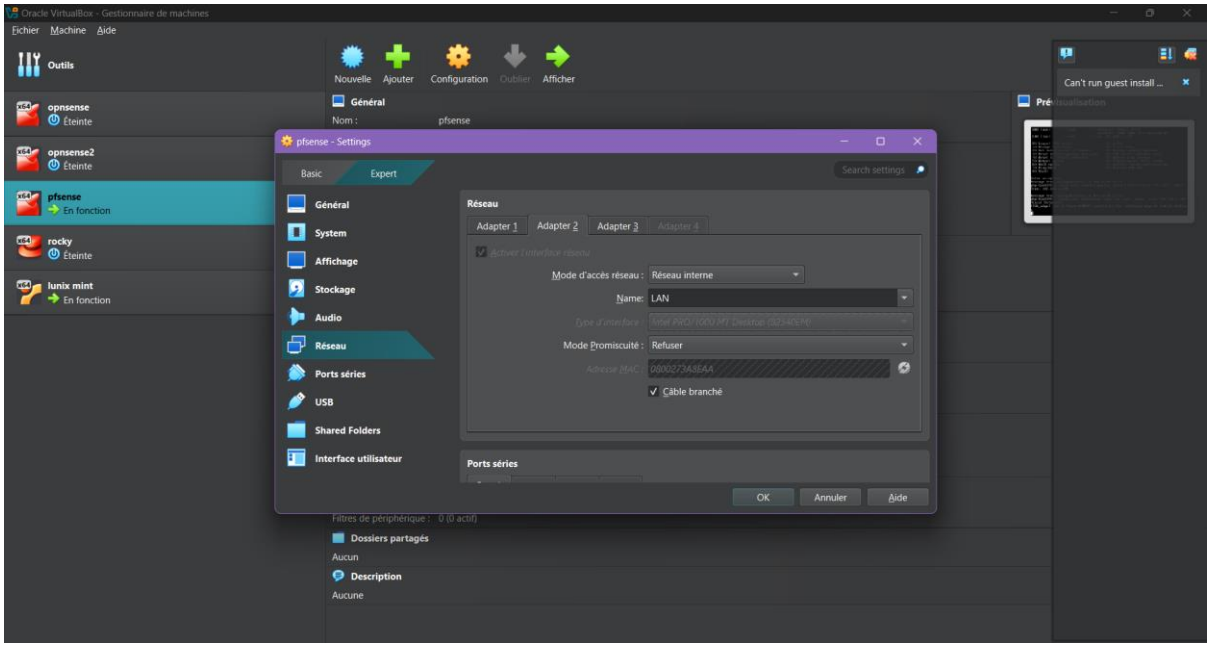
|\ ARICHITECTURE Réseau de base

Avant de commencé nous allons ouvrir nos machines virtuel pour pouvoir le TP de sécurité



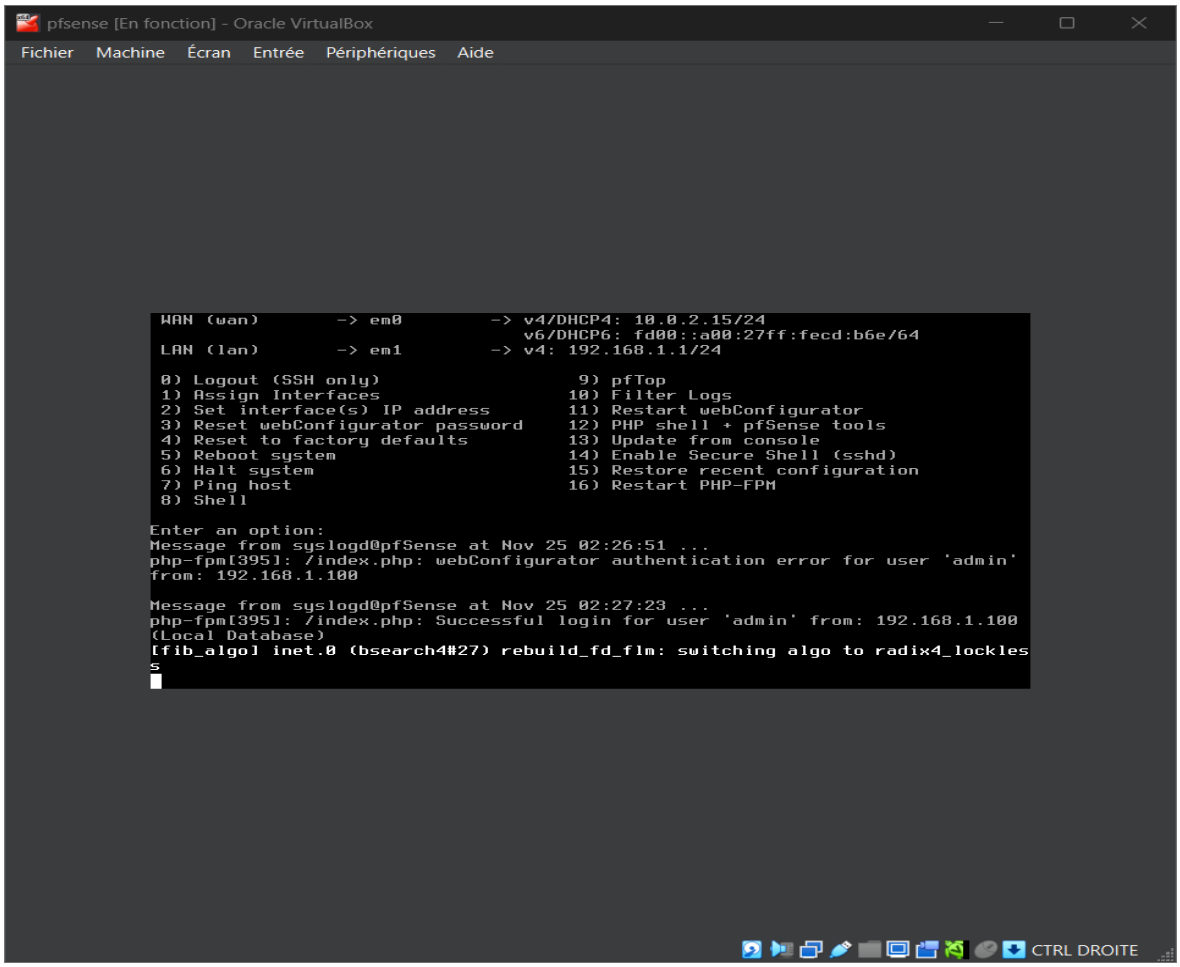
Nous allons mettre tous les réseaux en internes

- Réseau interne (LAN) :contient les postes de travail des utilisateurs 192.168.1.1/24
- WAN (réseau externe): Zone pour les services accessibles depuis l'extérieur(serveur web, serveur de messagerie, etc.) 10.0.2.15/24



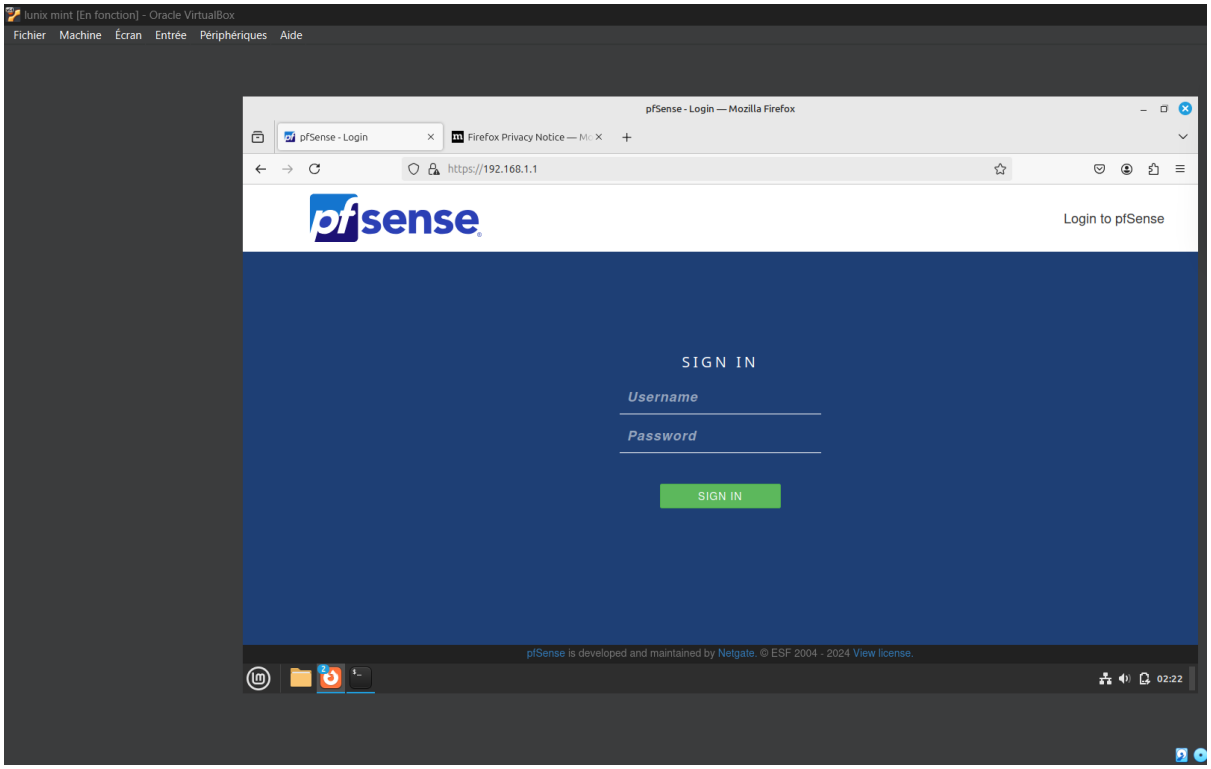
Le pare feu pf sense va être installé sur une machine dédié et sera connecté aux différents segments du réseau pour contrôler le trafic entrant et sortant

ON doit modifier les ip adresses assigné dans le pf sense



- Pf sense nous allons modifier les adresses ip si cela nous convient pas et aussi créer 3 cartes sous réseau pour le server
- Client : pour cette machine elle peut avoir 2 carte réseau
- Donc les deux outils doit
- Être en même réseau

.||/ Installation et configuration de pf sense

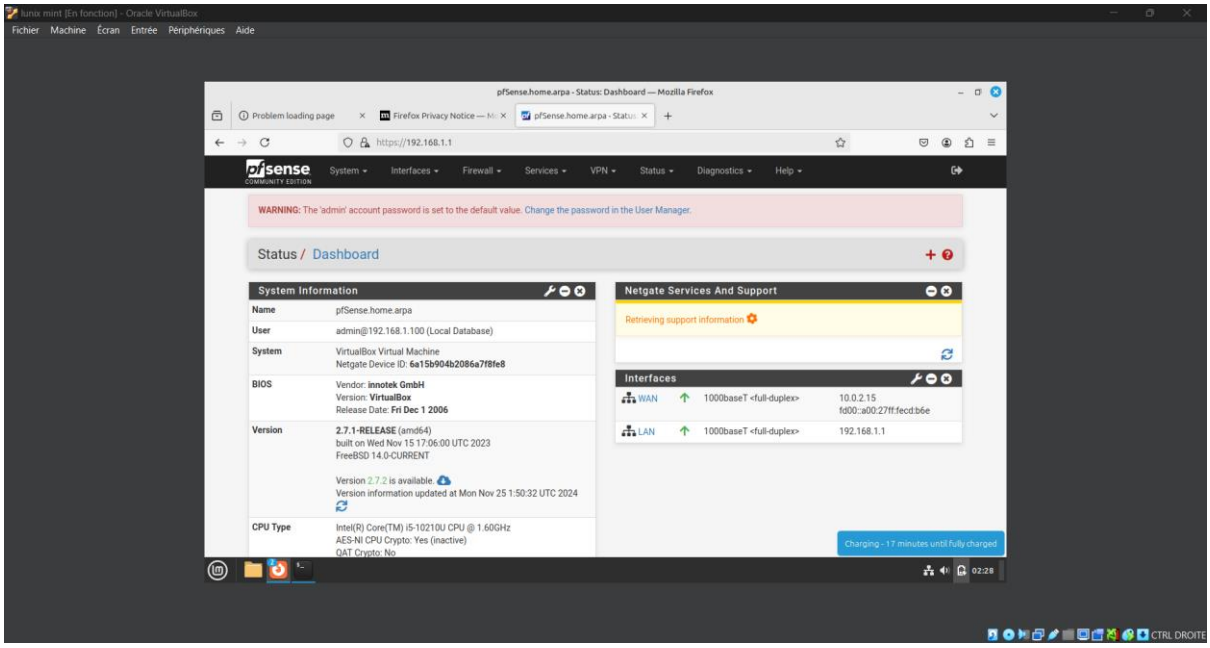


Voilà nous avons ouvert notre site dans le web de notre machine client pour pouvoir continuer le travail

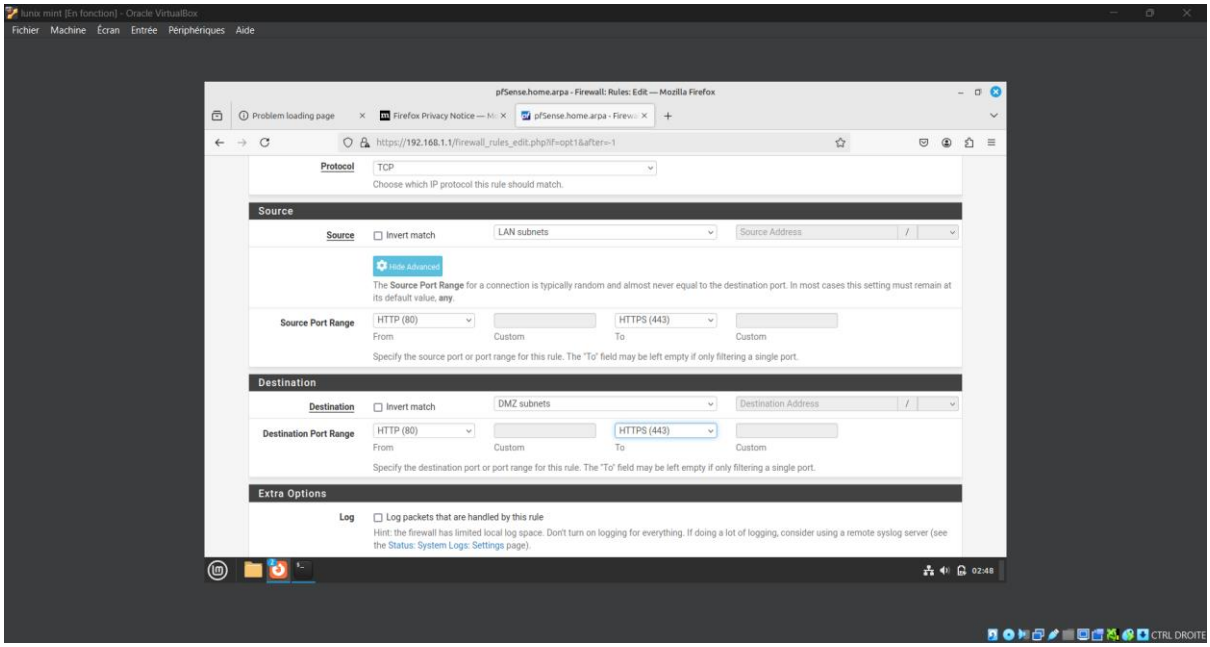
||| / Sécurisation du réseau avec des règles de filtrage

- D'abord nous allons vérifier les systèmes d'informations

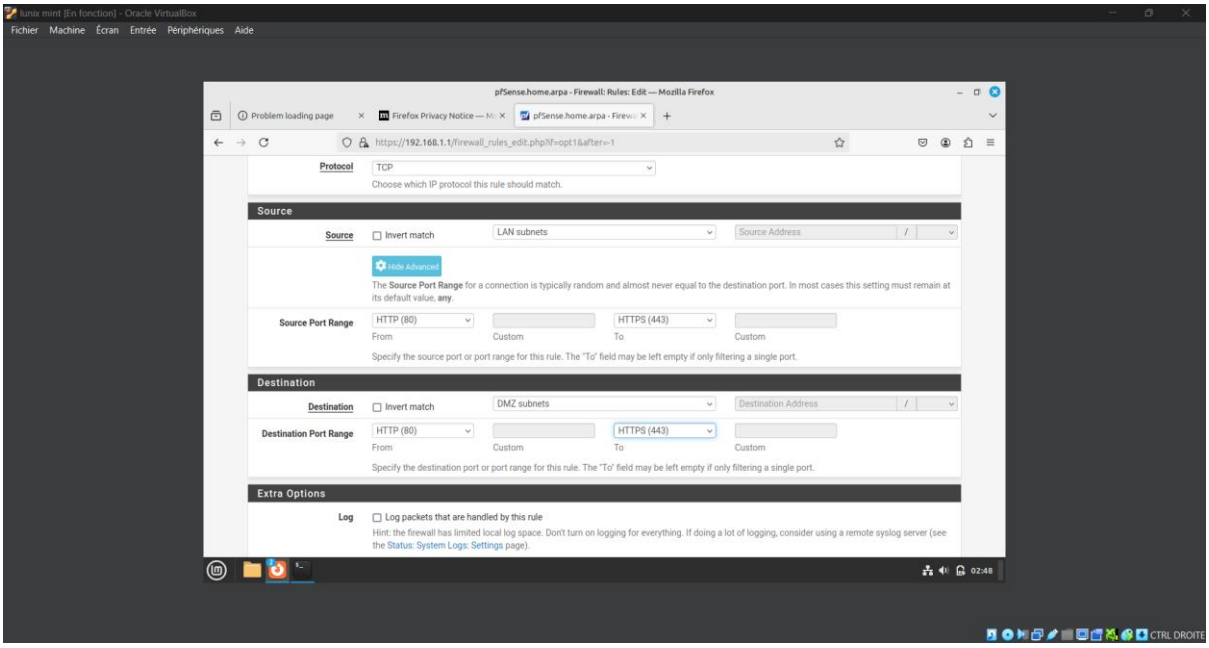
Création de règles de filtrage pour le LAN



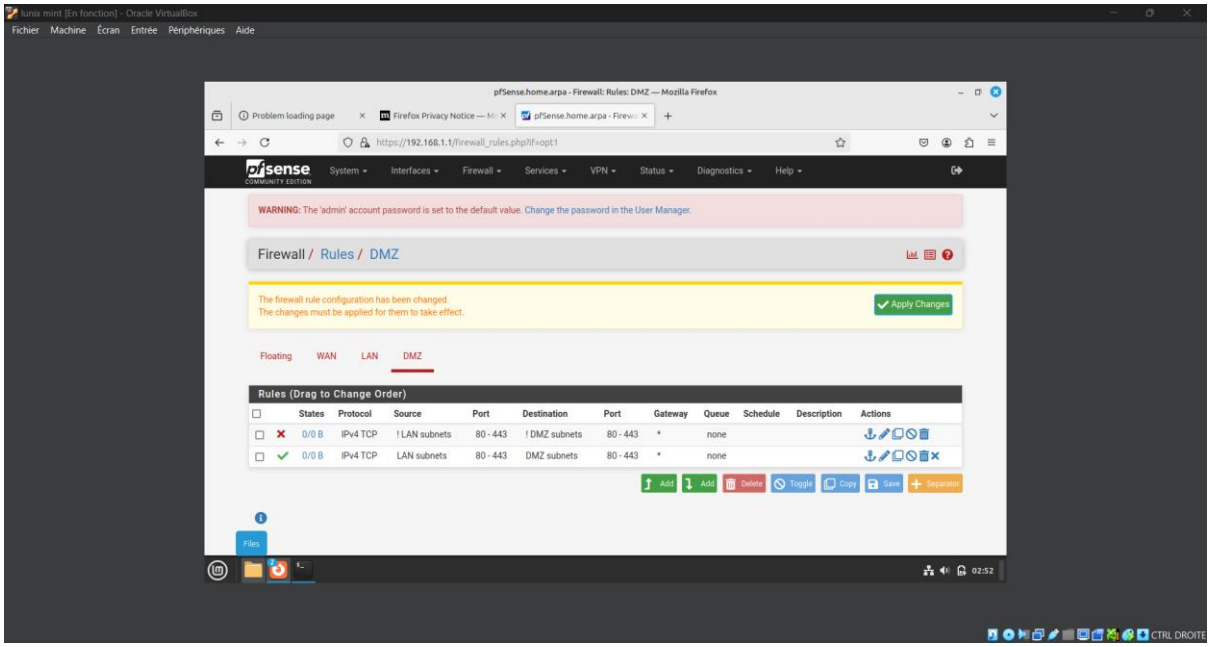
- Création de règles de filtrage pour le LAN



La Création de règles de filtrage pour le LAN • Allez dans Firewall > Rules > LAN. • Par défaut, pfSense autorise tout le trafic entrant et sortant sur le réseau LAN. Nous allons restreindre l'accès : o Créez une règle pour bloquer l'accès à Internet pour les utilisateurs du réseau LAN pendant les heures de travail (par exemple, du lundi au vendredi, de 9h00 à 18h00). o Créez une règle pour autoriser l’accès HTTP (port 80) et HTTPS (port 443) au serveur web dans la DMZ depuis le réseau LAN

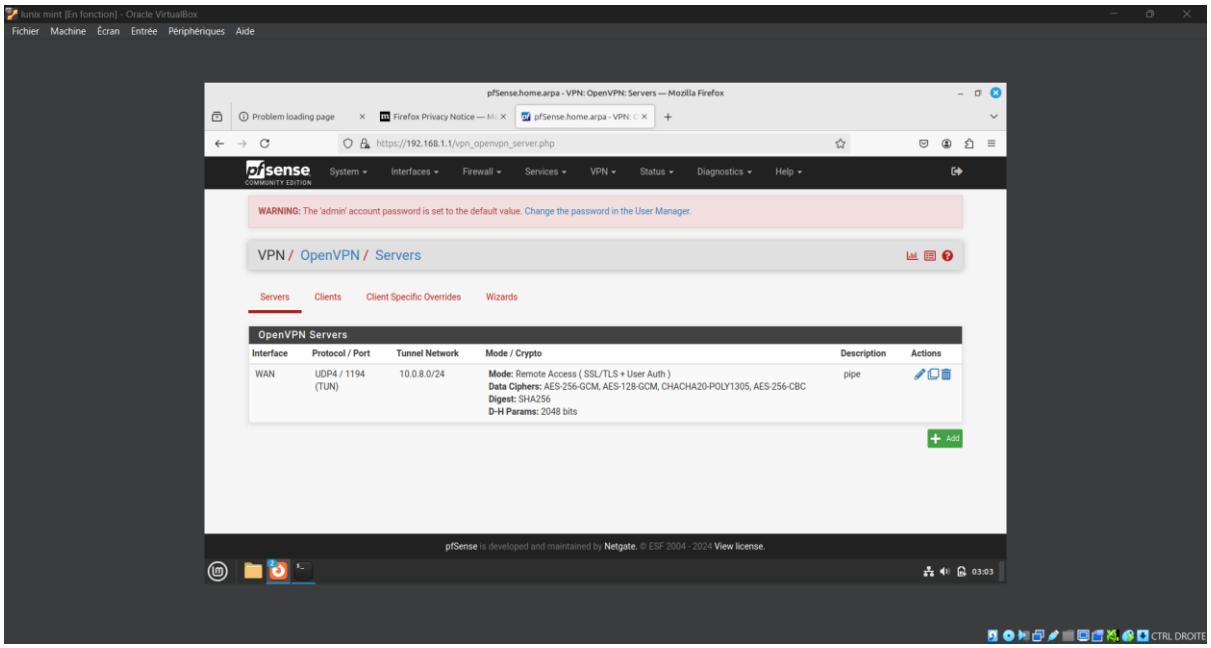


2. Filtrage entre le LAN et la DMZ



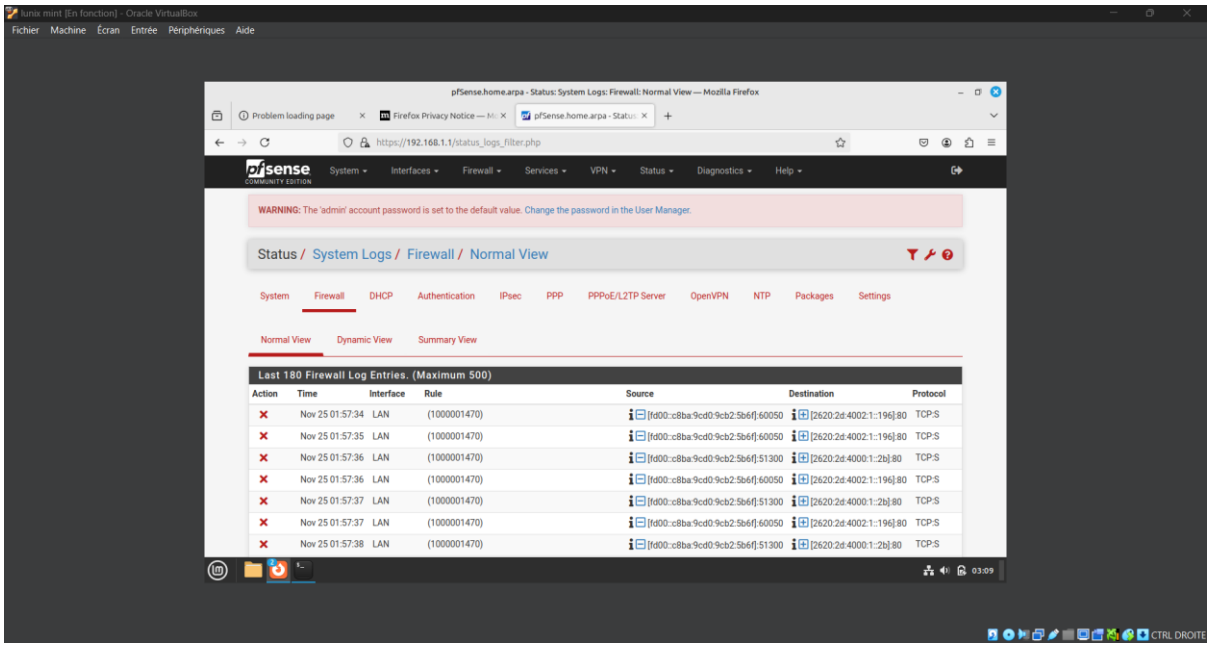
• Nous Allons dans Firewall > Rules > DMZ. • Autorisez uniquement le trafic HTTP/HTTPS depuis le WAN vers la DMZ pour permettre l'accès aux services web. • Bloquez tout autre trafic entrant sur la DMZ

4. Configuration d’un VPN



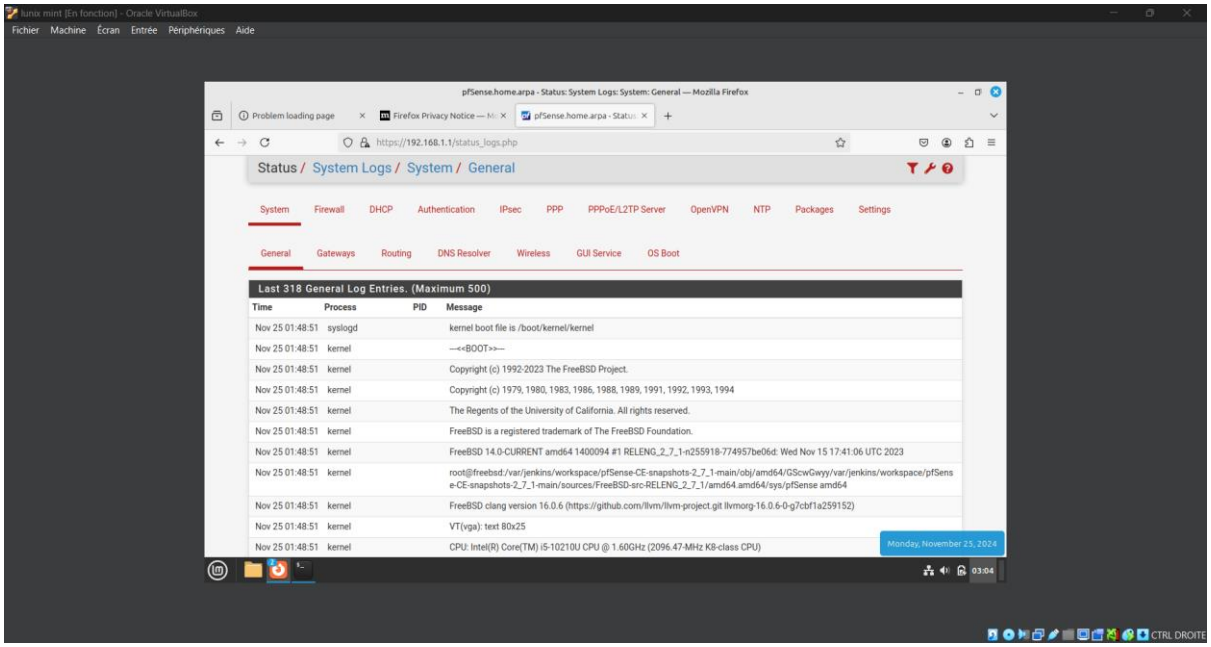
4.1. Configurons un VPN (OpenVPN) pour un accès sécurisé • Allez dans VPN > OpenVPN > Wizards pour configurer un serveur VPN. • Sélectionnez un certificat SSL (généralement, créez-en un si nécessaire). • Paramétrez les options pour un accès VPN sécurisé depuis l’extérieur, permettant à un utilisateur distant de se connecter à votre réseau interne de manière sécurisée.

4.2. Création de règles pour le VPN



Créons une règle sur Firewall > Rules > OpenVPN pour permettre le trafic VPN et autoriser l'accès au réseau interne via le tunnel sécurisé.

5. Surveillance et rapports



Nous Allons dans Status > System Logs pour surveiller les logs du pare-feu et vérifier si les règles fonctionnent comme prévu. • Activez les alertes dans System > Advanced pour être notifié des tentatives d'accès non autorisées.