Mise en place d'une solution pfSense afin de segmenter et de sécuriser le réseau d'une entreprise

Situation professionnelle 1

Nom : POSTIC

Prénom : Valentin

Classe : BTS SIO SISR

Année scolaire : 2025 - 2027

PICARD SURGELES

Plan de la situation

3. Cahier des charges

1.1. Expression des besoins

L’entreprise Z, composée d'une dizaine de collaborateurs répartis sur plusieurs services (Administration, Production, R&D, Invités), souhaite mettre en place une solution de routage et de sécurité réseau.
Elle souhaite segmenter son réseau en plusieurs VLANs distincts afin d'isoler les flux entre les différents services et limiter les risques de propagation en cas d'incident de sécurité. Chaque segment disposera de règles de filtrage précises contrôlant les communications inter-VLANs.

1.2. Description de l’existant

L’entreprise Z dispose pour le moment de la box fournie par son opérateur, connectée directement à l'ensemble des postes de travail et appareils mobiles. Aucun équipement réseau supplémentaire n'a été acquis. Tous les équipements (PC, imprimantes, smartphones) sont sur le même réseau sans aucune segmentation. Le Wi-Fi est partagé entre collaborateurs et visiteurs sans distinction.

1.3. Analyse des choix

Aucun équipement dédié :
Certaines petites structures démarrent sans aucun équipement réseau dédié, en s’appuyant uniquement sur le Cloud (Google Workspace, Microsoft 365). Simple à court

terme, il existe cependant un risque majeur : aucune maîtrise du réseau local, aucune protection des équipements internes.

Box du fournisseur d’accès à Internet :
La solution la plus simple : utiliser uniquement la box fournie par l’opérateur (Orange, SFR...). Elle intègre un routeur basique, un switch et le Wi-Fi. Zéro coût supplémentaire, mais aucune sécurité avancée, pas de segmentation, et des fonctionnalités très limitées. Acceptable uniquement pour 2-3 personnes sans données sensibles.

Commutateur manageable :
L’ajout d’un commutateur manageable (Cisco, HP, Netgear Pro...) permet de créer des VLANs pour segmenter le réseau sans forcément avoir un firewall avancé. Indispensable dès que l'entreprise grandit, il se couple idéalement avec un routeur ou pfSense.

Routeur professionnel :
Un routeur professionnel offre des fonctionnalités avancées : routage inter-VLANs, QoS, VPN, haute disponibilité. Plus fiable et performant qu'un routeur grand public, mais possède un coût plus élevé et nécessite une configuration technique plus poussée.

PfSense :
Solution firewall + routeur open-source déployable sur un mini-PC ou une VM. Elle offre une gestion complète : VLANs, VPN, IDS/IPS, portail captif, règles de filtrage avancées. Excellent rapport qualité/prix pour une petite entreprise souhaitant une vraie sécurité, moyennant quelques compétences techniques.

1.4. Solution retenue

Nous retiendrons ici la solution du pfSense afin de sécuriser et de segmenter le réseau de l'entreprise pour plusieurs raisons :

- Gestion des VLANs : permet de segmenter facilement le réseau en zones isolées (serveurs, utilisateurs, IoT, DMZ...) limitant la propagation des menaces latérales
- Firewall avancé : règles de filtrage granulaires entre chaque segment, avec contrôle précis des flux autorisés
- Coût maîtrisé : solution open-source, pas de licence, déployable sur du matériel standard ou en VM
- Interface web intuitive : administration centralisée et accessible, sans nécessiter de compétences CLI poussées
- Communauté & fiabilité : solution éprouvée, largement déployée en entreprise, avec des mises à jour régulières

2. Mise en oeuvre technique

2.1. Présentation du matériel utilisé

1. **Switch** : Cisco Catalyst 2960-S avec alimentation.
2. **PfSense**, comprenant :
    - Mini-tour
    - Écran
    - Support d'écran
    - Clavier
    - Câble HDMI
    - Câble d'alimentation

3. **Ordinateur portable** disposant d'un port Ethernet.

4. **Câble console** pour la connexion au switch.

5. **Trois câbles RJ45** pour les connexions réseau.

2.2 Présentation du logiciel utilisé

PuTTY est un logiciel client SSH, Telnet et Serial open-source et gratuit.

Il permet d'établir des connexions distantes sécurisées vers des équipements réseau ou des serveurs (routeurs, switches, serveurs Linux...) depuis un poste Windows, via les protocoles

Secure Shell pour les connexions chiffrées et sécurisées, ainsi que Serial pour les connexions directes via port COM.

PuTTY est gratuit et léger, ne nécessitant aucune installation car il se présente sous forme de simple exécutable. Son interface est minimaliste et intuitive, ce qui le rend simple d'utilisation. Il est très répandu dans le milieu de l'administration système et réseau. Il gère également les clés SSH pour une authentification sécurisée et permet la sauvegarde de profils de connexion pour un accès rapide aux équipements.

2.3. Préparation physique

Brancher l'alimentation du Switch sur une prise secteur et connectez-la au Switch. Brancher l'alimentation de la mini-tour sur une prise secteur. Installer l'écran sur pied, puis connecter le clavier via le port USB ainsi que l'écran via le câble HDMI à la mini-tour. Connecter un câble RJ-45 d'une prise réseau à la mini-tour sur le Port 1, correspondant au Port WAN. Connecter un câble RJ-45 de la mini-tour sur le Port 2, correspondant au LAN, jusqu'au Switch sur l'un des ports prévus à cet effet (ici, le port choisi est le port 20).

Il est important de vérifier l'état du matériel utilisé, notamment l'état des câbles.

Il est également fortement conseillé de vérifier les ports du switch avant de réaliser une quelconque action (pour cela, brancher le câble console à l'ordinateur portable et relier le au switch : aller sur Putty et entrer les commandes "en" et "show run" afin de vérifier les ports utilisés ou non par le switch et ainsi d'éviter toute confusion).

2.4. Configuration du Pfsense

Appuyer sur le bouton “Power” de la mini-tour. Une fois le système du Pfsense démarré, il est nécessaire de configurer le WAN ainsi que le LAN afin de pouvoir récupérer Internet.

Configuration du WAN :

- Appuyer sur “2 : Set interface IP address“, puis sur “1 : WAN”

A partir de là, suivre la configuration suivante :

1. “Configure IPv4 address WAN interface via DHCP ?” => répondre “y” pour oui
2. “Configure IPv6 address WAN interface via DHCP ?” => répondre “n” pour non
3. “Configure IPv4 address WAN interface via DHCP ?” => Appuyer sur “entrée”
4. Une fois le système mis à jour, appuyer à nouveau sur “entrée”

L’écran d’accueil affiche une adresse IPv4 sur la ligne “WAN igc0” (ici “192.168.1.47”).

Il est très fortement conseillé de vérifier la connectivité du PfSense en saisissant l’option “7 : Ping host” et de rentrer l’adresse IPv4 suivante : “8.8.8.8” (adresse du serveur DNS).

Pour la configuration du LAN :

- Appuyer sur “2 : Set interface IP address”, puis sur “2 : LAN”

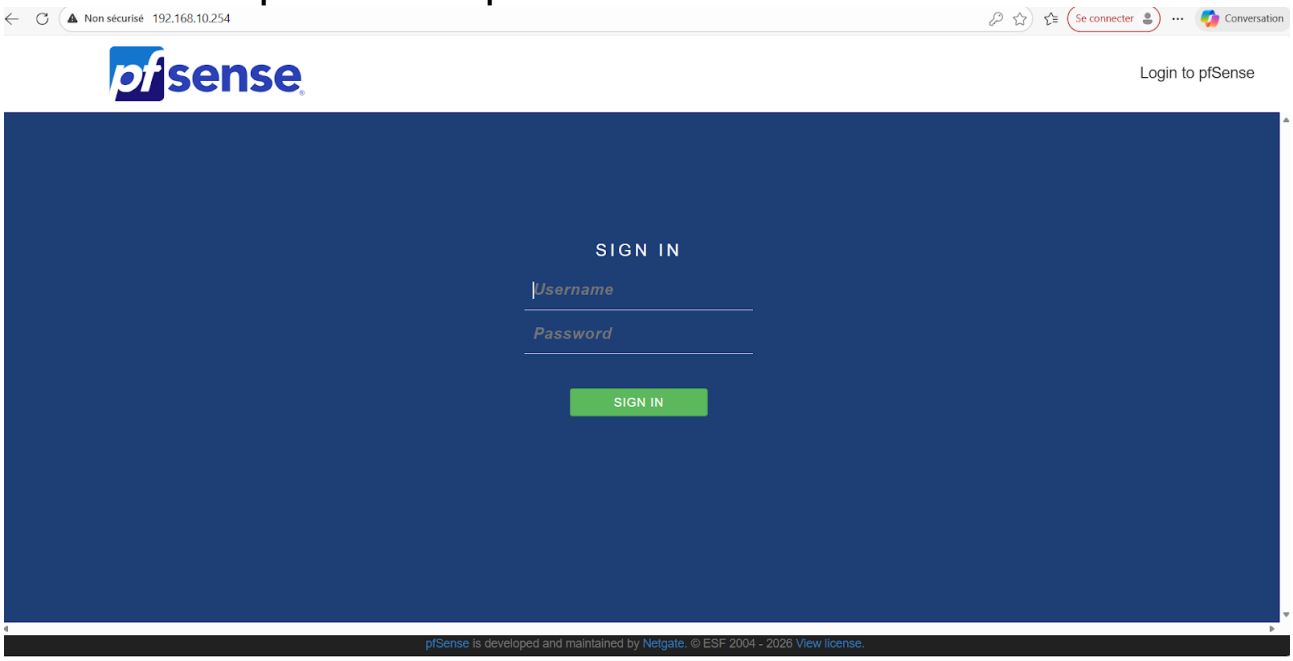
A partir de là, suivre la configuration suivante :

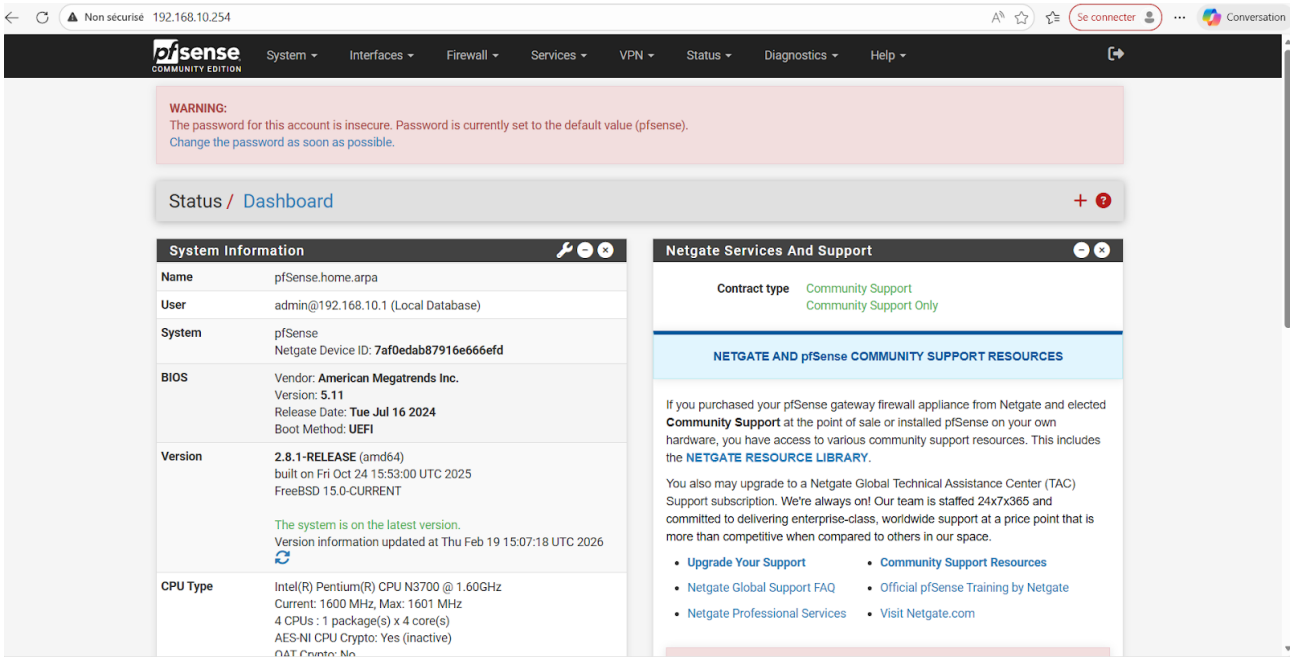
1. “Configure IPv4 address LAN interface via DHCP ?” => répondre “n” pour non
2. “Enter the new LAN IPv4 address” => entrer l’adresse IPv4 “192.168.10.254”

3. “Enter the new LAN IPv4 subnet bit count” => répondre “24”
4. Appuyer sur “entrée”
5. “Configure IPv6 address LAN interface via DHCP ?” => répondre “n” pour non
6. Appuyer sur “entrée”
7. “Do you want to enable DHCP server on LAN” => répondre “y” pour yes
8. Entrer “192.168.10.1” comme adresse IPv4 de début
9. Entrer “192.168.10.253” comme adresse IPv4 de fin
10. Un affichage indiquant que l’on peut maintenant accéder à l’interface du PfSense via un navigateur web apparait avec l’adresse IPv4 “192.168.10.254”
11. Appuyer sur “entrée”

L’écran d’accueil affiche une adresse IPv4 sur la ligne “LAN igc1” (ici “192.168.10.254”)

Aller sur un navigateur web via l’ordinateur portable et entrer l’adresse IP “192.168.10.254”. Le site PfSense est chargé et un code est requis : par défaut le nom d’utilisateur est “admin” et le mot de passe est “pfsense”.

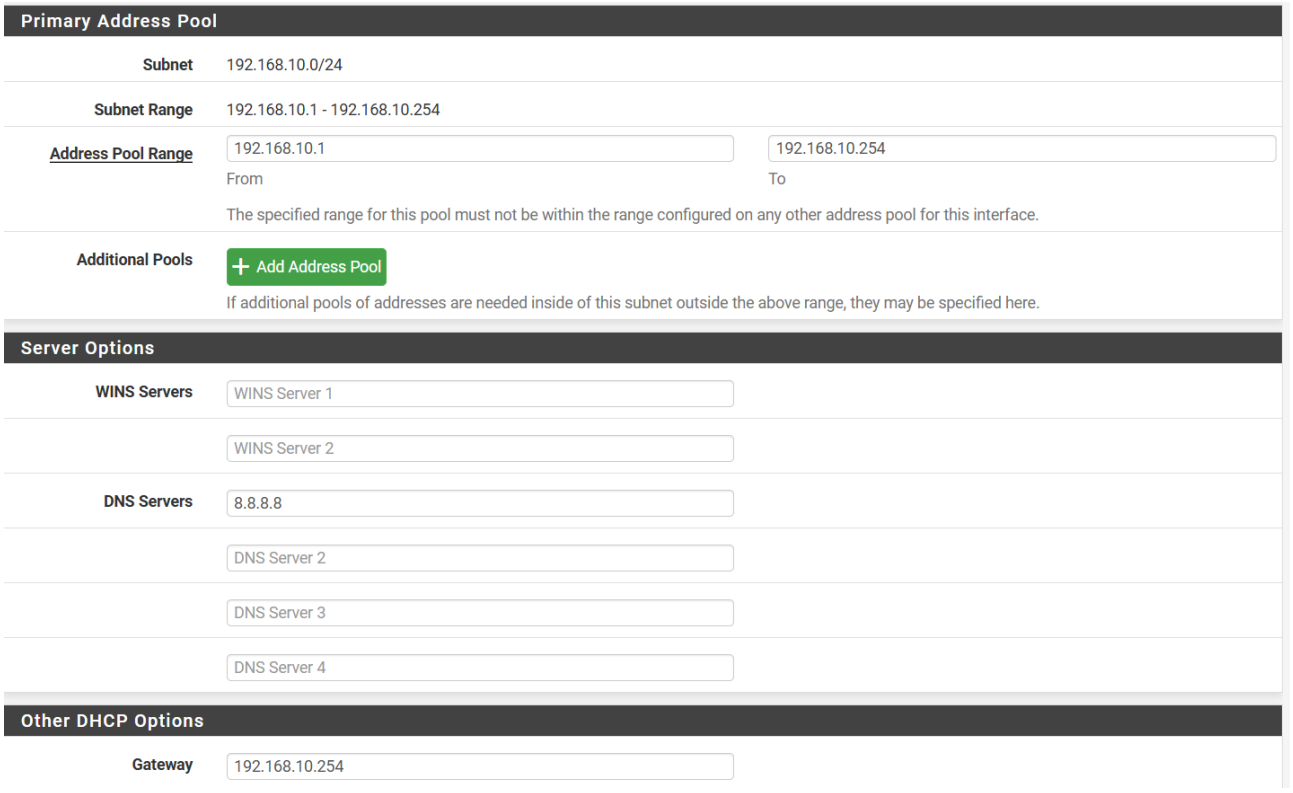




Une fois arrivé sur la page d'accueil de l'interface web :

- aller dans l'onglet "Services" puis cliquer sur "DHCP Server" :

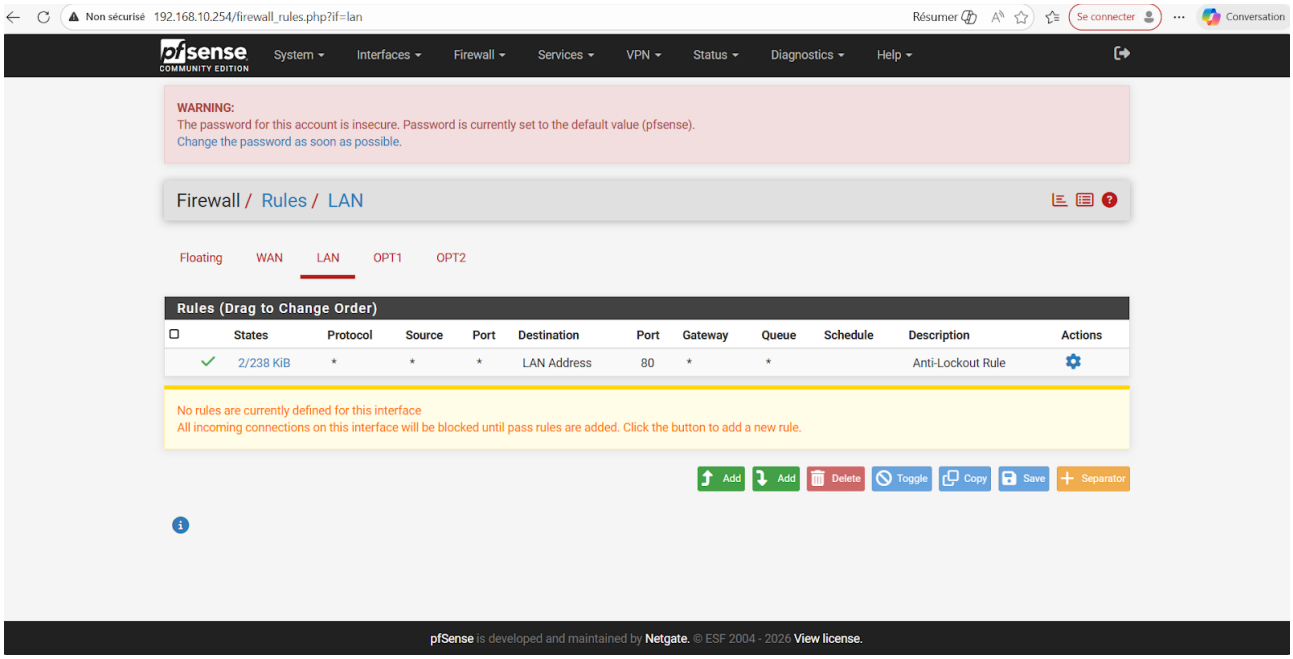
Cocher la case : "Enable DHCP server on LAN interface" et entrer les informations comme présenté ci-dessous.

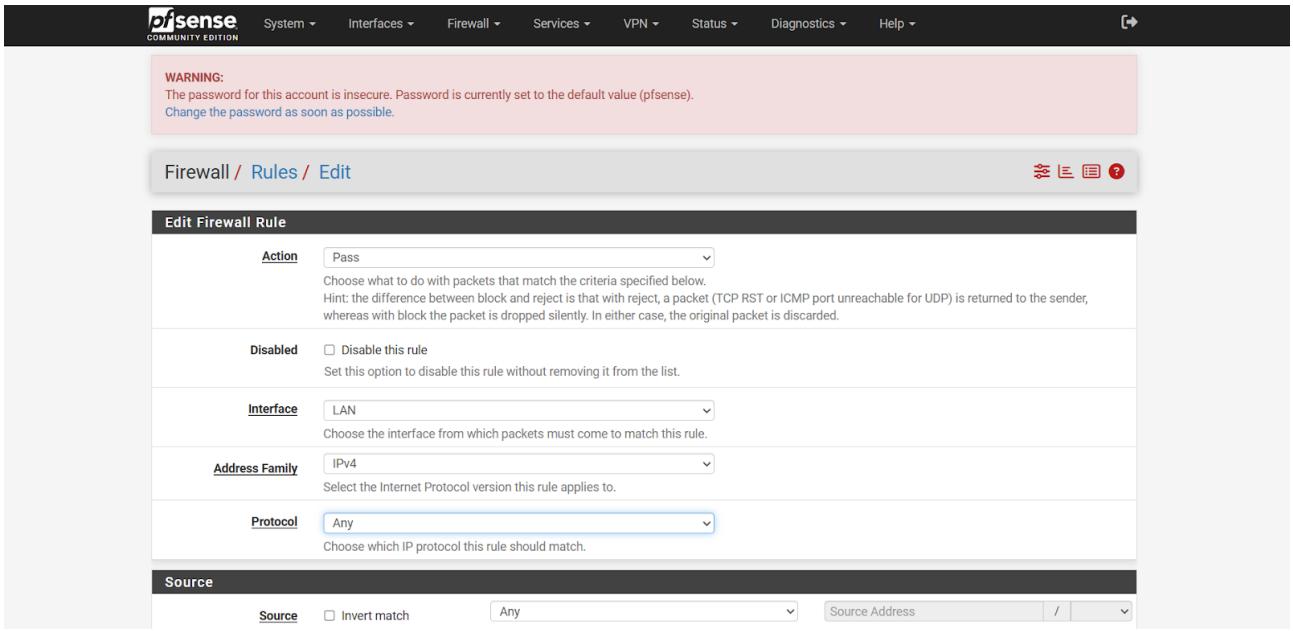


Attention : Bien penser à sauvegarder toute modification afin qu'elle soit bien prise en compte !

- aller dans l'onglet "Firewall" puis cliquer sur "Rules" :

Cliquer sur la case "Add" la plus à gauche puis dans la case "protocol" saisir l'option "Any"





2.5. Test et validation

Brancher l'ordinateur avec un câble RJ-45 sur l'un des ports du switch et vérifier que l'ordinateur portable récupère bien internet.

Il est également important de réaliser un "ipconfig", "ipconfig / release" ainsi que "ipconfig /renew" afin de connaître son adresse IPv4, et le cas échéant demander une nouvelle adresse IPv4 au serveur DHCP.