Projet Personnel : Lab Virtuel

Lab [1] : Création d'un lab avec Pfsense, WAN + LAN + DMZ

Auteur :

Angel VELASCO

Paris, le 02/08/2025

I. Introduction

Dans le cadre de ce projet, j'ai conçu un **laboratoire virtuel sécurisé** en utilisant **pfSense** comme pare-feu principal. L'objectif était de mettre en place une architecture réseau réaliste composée de trois zones distinctes :

- Une interface **WAN** simulant une connexion à Internet,
- Une interface **LAN** dédiée aux machines internes et utilisateurs,
- Et une **DMZ** (zone démilitarisée) destinée à héberger un **serveur web** accessible depuis l'extérieur.

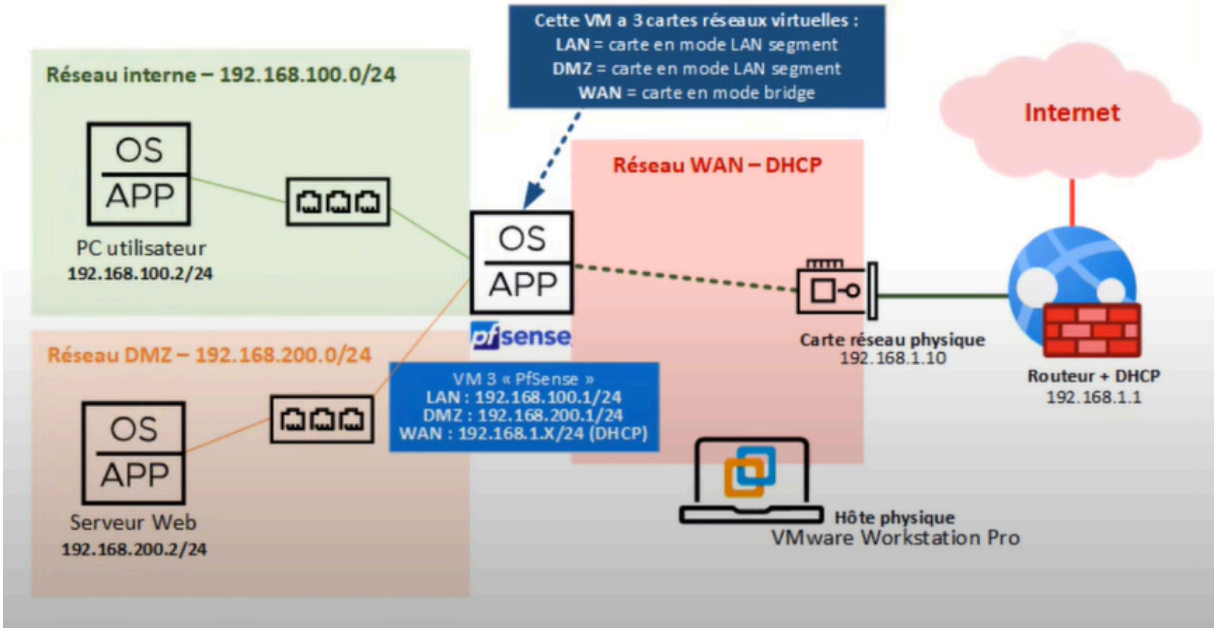
Ce projet permet d'acquérir une meilleure compréhension de la segmentation réseau, des règles de pare-feu, du NAT et de la gestion des flux dans un environnement sécurisé.

II. Schéma du Lab

Dans cette section, je vais présenter l'architecture réseau que j'ai mise en place dans mon laboratoire virtuel. J'ai utilisé une machine virtuelle **pfSense** comme cœur du système, à laquelle j'ai associé trois interfaces réseau distinctes, correspondant aux trois zones de sécurité classiques : **WAN**, **LAN** et **DMZ**.

La VM pfSense est connectée à :

- une interface **WAN** en mode *bridge* (simulant Internet),
- une interface **LAN** (réseau local interne),
- une interface **DMZ** (zone démilitarisée).



- **Schéma du réseau**

Afin de mieux comprendre le but de ce Lab voici une explication de chaque interface réseau utilisé.

WAN (Wide Area Network)

L'interface **WAN** représente la connexion à Internet. Dans mon cas, j'ai configuré cette interface en **mode bridge** dans VirtualBox, ce qui permet à pfSense de récupérer automatiquement une adresse IP publique depuis mon **routeur personnel** (via DHCP).

- **But** : Simuler un accès Internet réel pour tester des règles de NAT, d'accès externe, etc.
- **Exemple IP** : `192.168.1.16` (attribuée automatiquement par le routeur de mon réseau local)
- **Risque** : L'accès WAN est considéré comme non fiable – c'est de là que peuvent venir les attaques externes.

LAN (Local Area Network)

Le **LAN** est le réseau interne, dédié aux machines de confiance (par exemple : PC utilisateur, outils d'administration, etc.). Dans mon lab, j'y ai connecté un PC Windows 11. Cette interface est configurée en **réseau interne isolé** (Internal Network), pour qu'elle ne puisse communiquer qu'avec pfSense.

- **But** : Zone protégée ; accès autorisé vers Internet et vers certains services de la DMZ.
- **IP du client LAN** : `192.168.100.2`

DMZ (Demilitarized Zone)

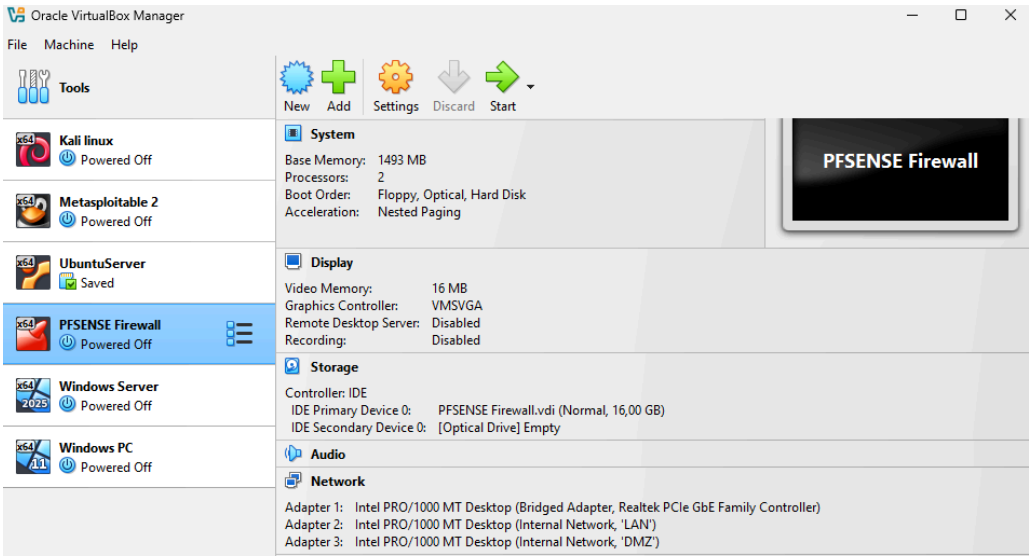
La **DMZ** est une zone intermédiaire entre le WAN et le LAN. Elle accueille des **services exposés** à Internet, comme un **serveur web** dans mon cas. Cette zone est aussi en **réseau interne isolé** pour la maintenir séparée du LAN.

- **But** : Permettre l'accès public à un service tout en protégeant le reste du réseau.
- **IP du serveur Web (Windows Server 2025)** : `192.168.200.2`
- **Sécurité** : La DMZ ne peut pas communiquer librement avec le LAN ; seules certaines règles de pare-feu le permettent (par exemple HTTP ou HTTPS depuis LAN vers DMZ).

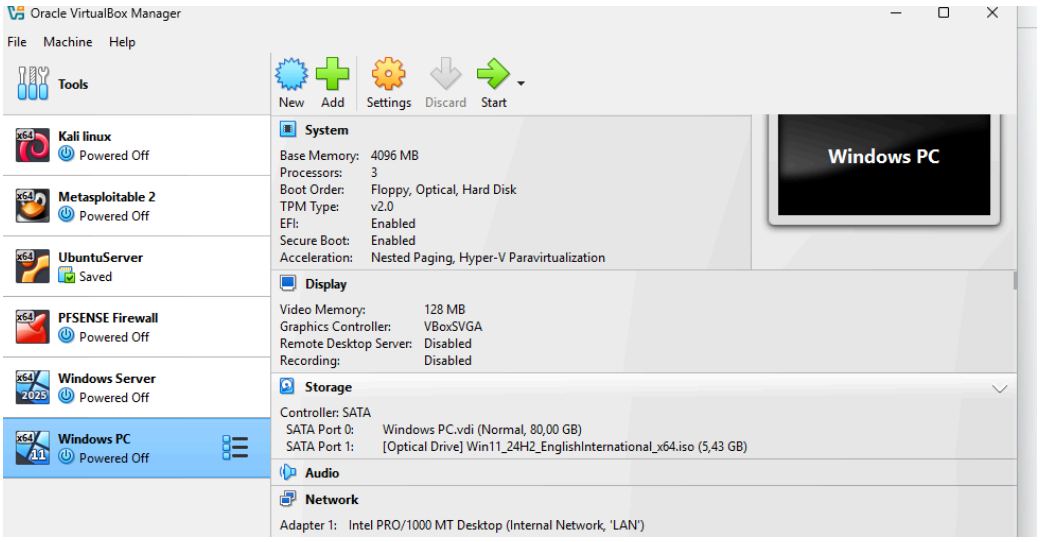
III. Installation des Machines Virtuelles

Pour créer mon laboratoire, j'ai utilisé VirtualBox comme hyperviseur. J'ai créé trois machines virtuelles :

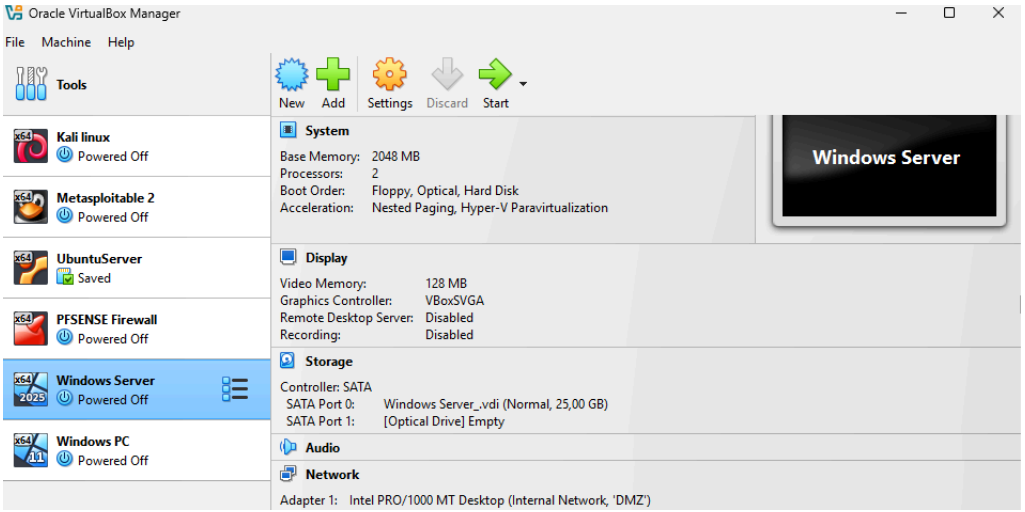
1. Une VM pfSense qui fera office de pare-feu et de routeur central,
2. Une VM Windows 11 connectée au LAN,
3. Une VM Windows Server 2025 dans la DMZ, configurée comme serveur web.



- Capture d'écran de la configuration de Pfsense



- Capture d'écran de la configuration de Windows 11



- Capture d'écran de la configuration de Windows server 2025

IV. Configurer pfSense : les interfaces réseau (LAN et WAN)

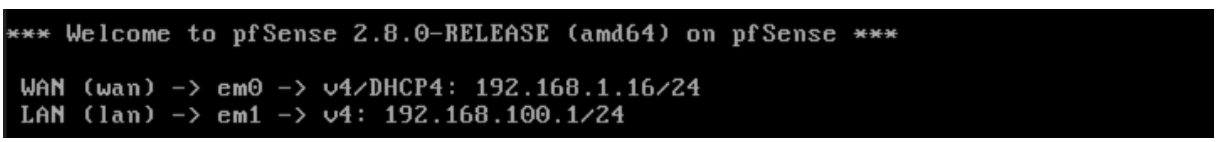
Une fois la VM pfSense démarrée pour la première fois, j'ai accédé à son interface en **mode console texte** pour configurer manuellement les interfaces réseau.

Interface WAN

- Lors du démarrage, pfSense détecte automatiquement une IP sur l'interface **WAN**, car elle est en mode **Bridge**.
- Mon routeur local lui a attribué une **adresse IP via DHCP** :
  - Exemple : `192.168.1.16`
- Cela signifie que la connexion Internet simulée (depuis mon réseau domestique) fonctionne déjà correctement.

Interface LAN (réseau interne)

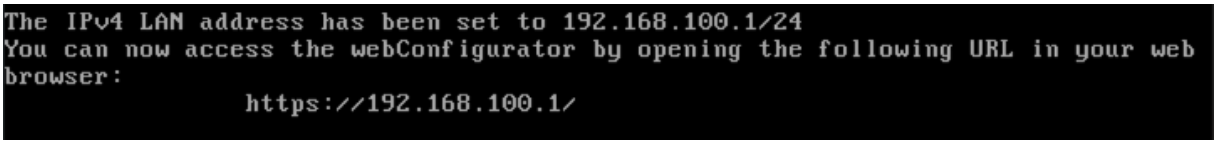
L'interface **LAN** est dédiée aux machines internes de confiance (comme un client Windows ou un poste administrateur). Par défaut, pfSense lui attribue une IP de type `192.168.1.1`, mais j'ai choisi de **modifier cette adresse** pour qu'elle corresponde à mon plan d'adressage initial.



- capture console pfSense montrant l'IP WAN & LAN

Accès à l'interface Web de pfSense

Une fois ces réglages effectués, pfSense m'indique que je peux désormais accéder à son interface Web depuis un navigateur, via l'adresse :

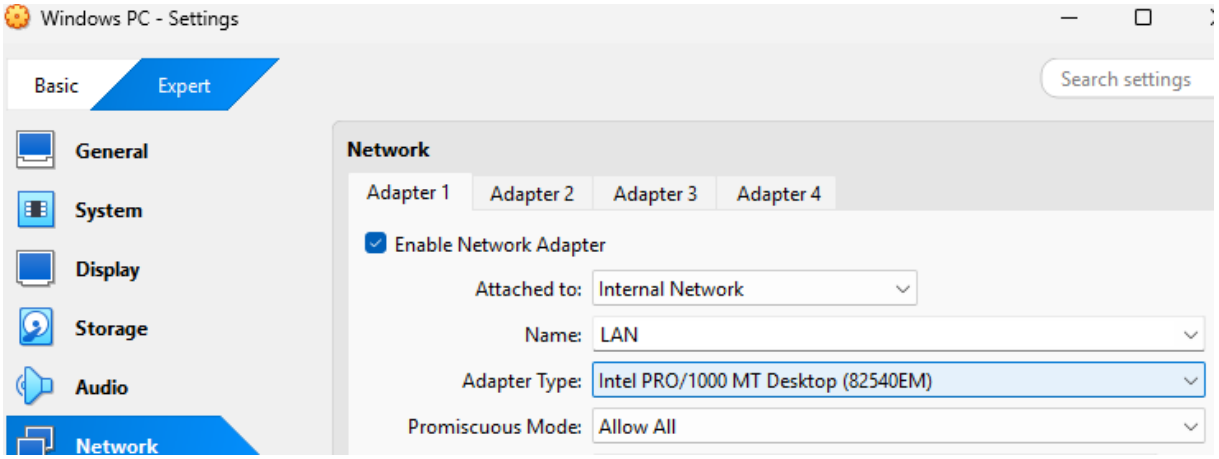


- capture console pfSense montrant l'Adresse Web

La prochaine étape consiste à **ajouter et configurer la DMZ**, qui viendra se placer comme une zone tampon entre Internet (WAN) et mon réseau sécurisé (LAN).

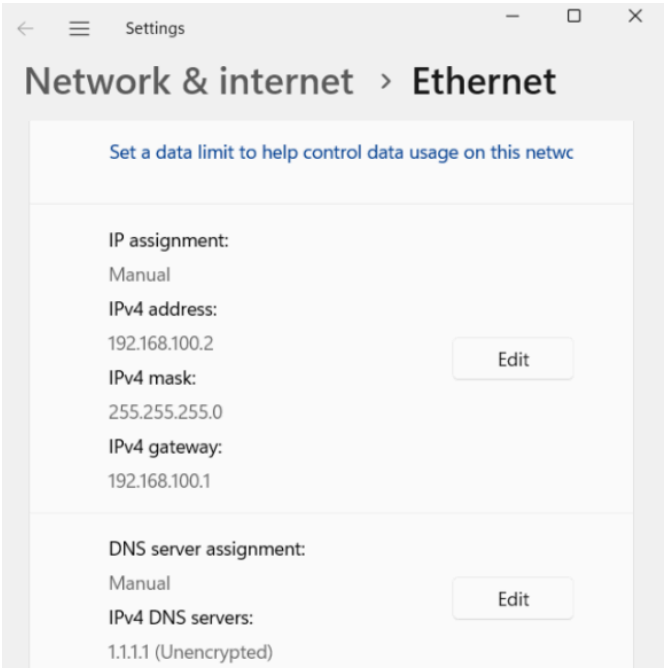
V. Se connecter à pfSense et créer la DMZ

Une fois les interfaces WAN et LAN configurées, j'ai lancé ma machine cliente (Windows 11) pour accéder à l'interface d'administration de pfSense. Par défaut, l'adaptateur réseau de la VM était configuré en mode NAT. J'ai modifié ce paramètre pour l'assigner au même **LAN segment** que pfSense, afin que la machine cliente soit bien dans le sous-réseau LAN `192.168.100.0/24`.



- Paramétrage du LAN segment dans VirtualBox

Comme je n'avais pas activé de serveur DHCP sur l'interface LAN de pfSense, j'ai configuré une **adresse IP statique** sur la machine cliente (par exemple `192.168.100.2`), avec `192.168.100.1` comme passerelle et serveur DNS.



- Configuration IP statique sur Windows

Ensuite, j'ai ouvert un navigateur et accéder à pfSense via `https://192.168.100.1`. Comme attendu, le certificat étant auto signé, une alerte de sécurité s'est affichée, que j'ai ignorée pour continuer. Je me suis connecté avec les identifiants.

Ajout et configuration de l'interface DMZ

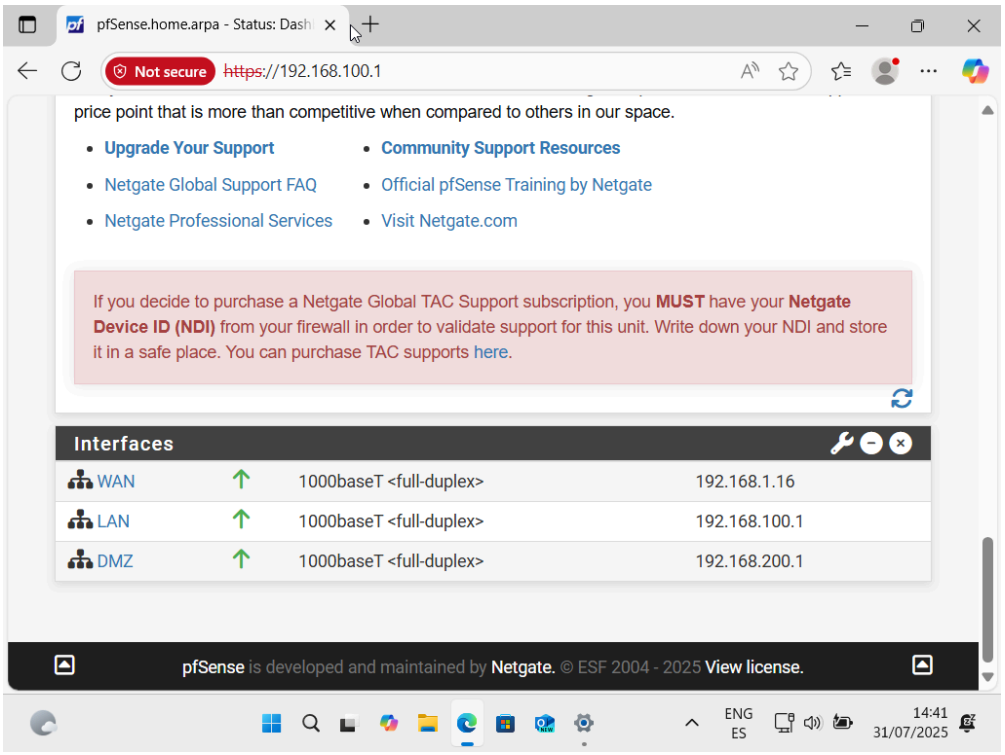
Je suis ensuite allé dans le menu `Interfaces > Assignments` pour ajouter une troisième interface réseau à pfSense, destinée à la **DMZ**. Cette interface apparaissait comme disponible (non assignée), je l'ai ajoutée puis activée.

Je l'ai renommée **DMZ**, puis configurée en **adresse IP statique** avec :

- Adresse IP : `192.168.200.1`
- Masque : `/24`

Une fois les changements appliqués, pfSense affichait bien trois interfaces actives :

- **WAN** (vers Internet),
- **LAN** (réseau interne),
- **DMZ** (zone démilitarisée pour services exposés comme le serveur web).



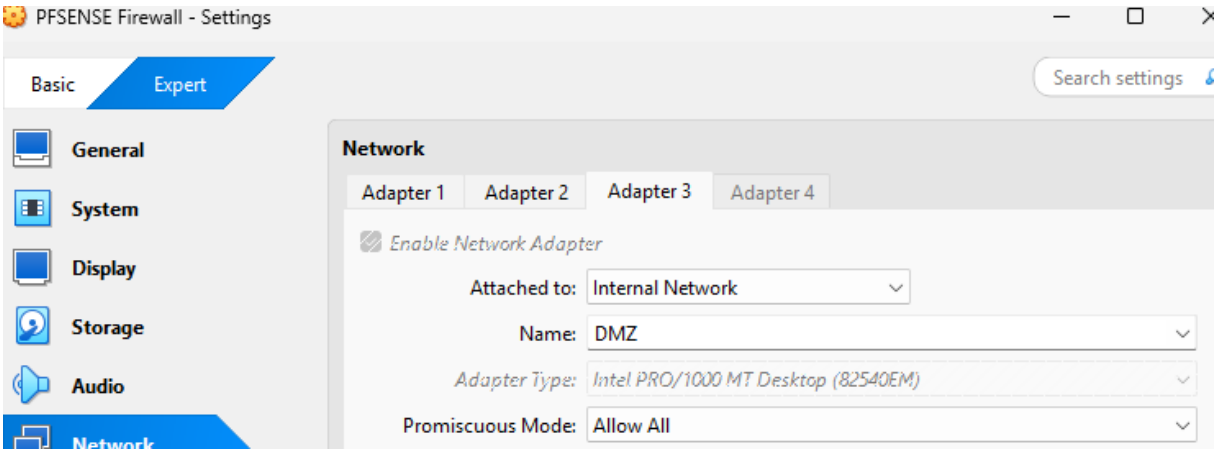
- Tableau de bord avec 3 interfaces UP

Je suis désormais prêt à configurer la sécurité réseau via les **règles de pare-feu** et la **règle NAT** pour permettre un accès contrôlé au serveur Web en DMZ.

VI. Configurer le serveur Web (en DMZ)

Pour héberger un site web dans une zone sécurisée, j'ai utilisé Windows Server 2022 que j'ai configuré comme serveur Web IIS, placé dans le sous-réseau DMZ.

J'ai commencé par modifier la configuration réseau de la machine virtuelle sur VirtualBox, en la connectant au LAN segment DMZ (identique à l'interface DMZ de pfSense).



- Configuration du LAN segment "DMZ" dans VirtualBox

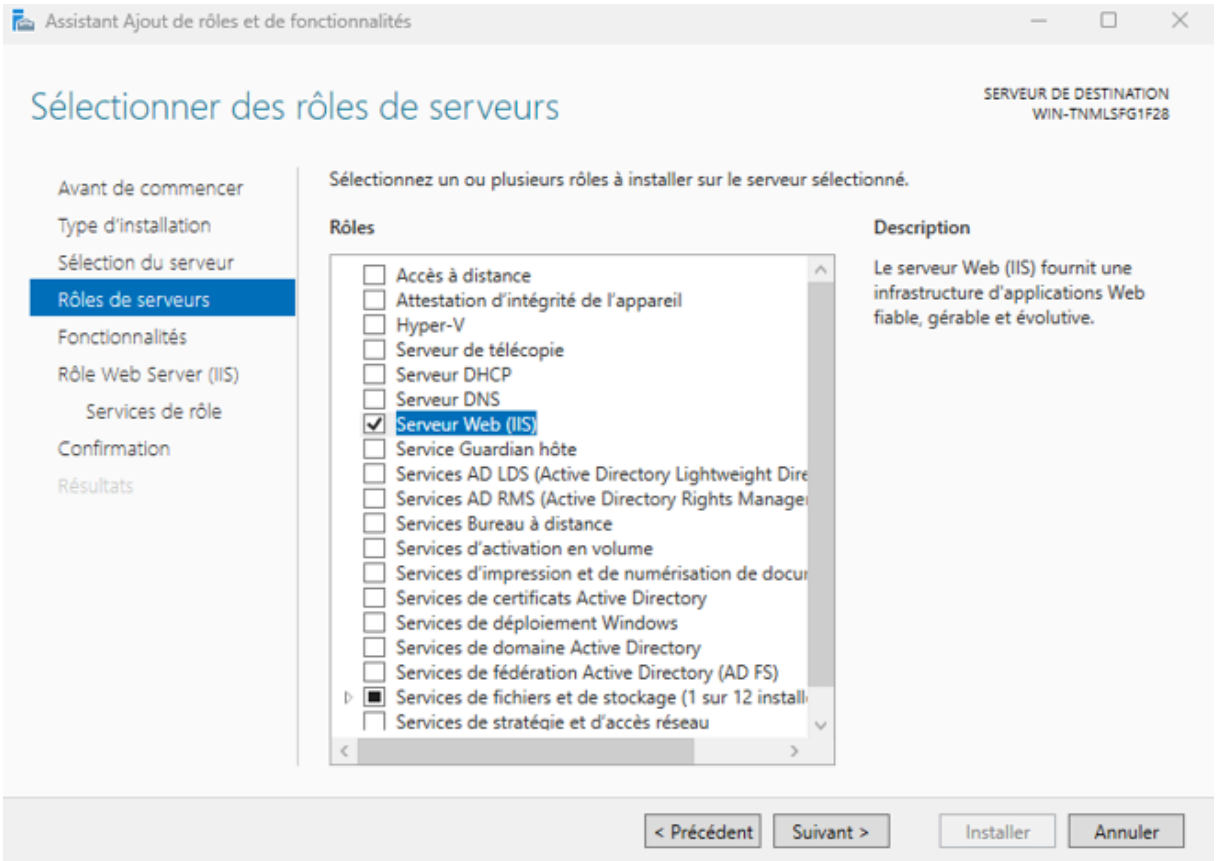
Une fois la VM démarrée, je lui ai attribué une adresse IP statique dans le réseau DMZ :

- IP : `192.168.200.2`
- Masque : `255.255.255.0`
- Passerelle : `192.168.200.1` (interface DMZ de pfSense)

Installation du rôle IIS sur Windows Server 2022

Une fois le serveur connecté au bon réseau, j'ai installé le rôle IIS (Internet Information Services) via le Gestionnaire de serveur :

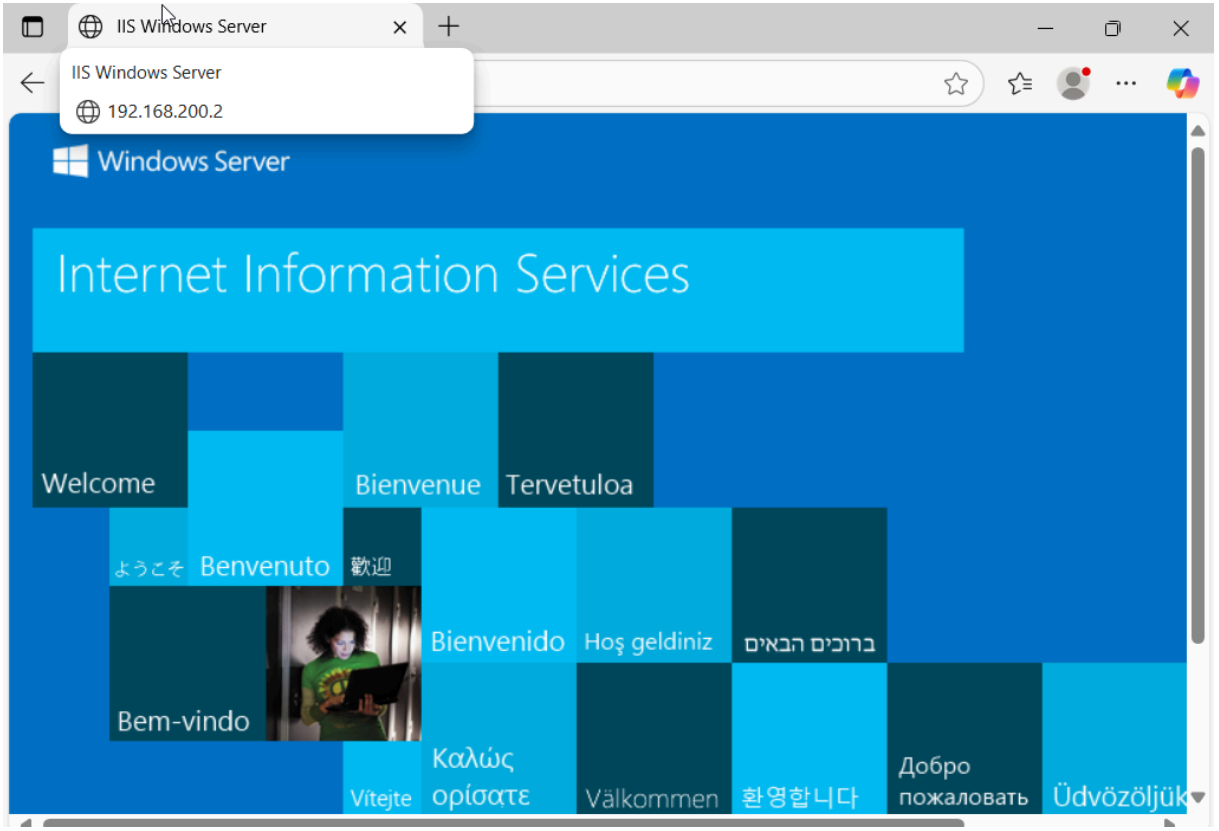
- J'ai cliqué sur "Ajouter des rôles et fonctionnalités"
- J'ai sélectionné le rôle "Serveur Web (IIS)"
- J'ai accepté les fonctionnalités associées par défaut
- J'ai laissé les options de base (HTTP uniquement), suffisantes pour héberger une simple page web



- *Assistant ajout de rôle IIS*

Accès depuis le LAN (client interne)

Depuis mon poste client Windows 11 dans le réseau LAN, j'ai saisi l'adresse IP du serveur `http://192.168.200.2` dans un navigateur. Grâce aux règles par défaut sur l'interface LAN (qui permettent tous les flux sortants), j'ai pu accéder au serveur Web en DMZ sans restriction.



- Accès à la page IIS depuis le poste client LAN

À ce stade, l'accès fonctionne uniquement depuis le LAN. Pour l'ouverture depuis le WAN (Internet), je devrai ensuite créer une règle NAT et un filtrage firewall adapté, que je détaillerai dans la section suivante.

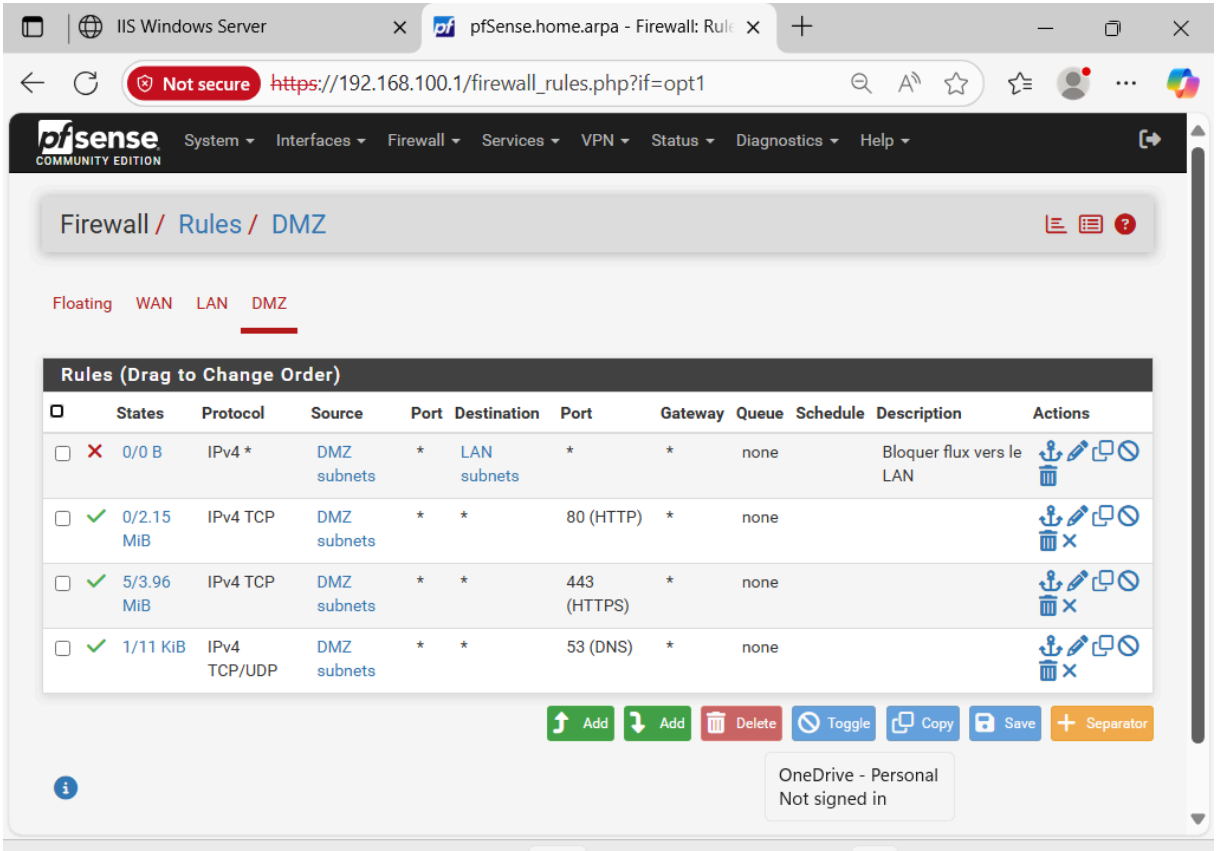
VII. Configurer les règles Firewall

Pour garantir l'isolation et la sécurité de chaque zone de mon lab, j'ai défini des règles précises sur les interfaces **DMZ** et **LAN** de pfSense.

Interface DMZ

Sur l'interface **DMZ**, ma première préoccupation a été d'empêcher tout trafic en provenance de la zone démilitarisée vers le réseau interne. Pour cela, j'ai créé une règle bloquant **tous les protocoles** entre la source « DMZ subnets » et la destination « LAN subnets » (voir capture ci-dessous). Cette mesure garantit qu'un éventuel serveur compromis ne puisse pas se retourner contre mes machines internes.

Ensuite, j'ai besoin que mon serveur web en DMZ puisse accéder à Internet pour récupérer des mises à jour ou interagir avec des API externes. J'ai donc ajouté trois règles autorisant respectivement le trafic **HTTP (port 80)**, **HTTPS (port 443)** et **DNS (port 53)** en sortie vers n'importe quelle destination. Le choix de restreindre ces flux uniquement à ces protocoles minimise la surface d'attaque tout en préservant les fonctionnalités essentielles du serveur.

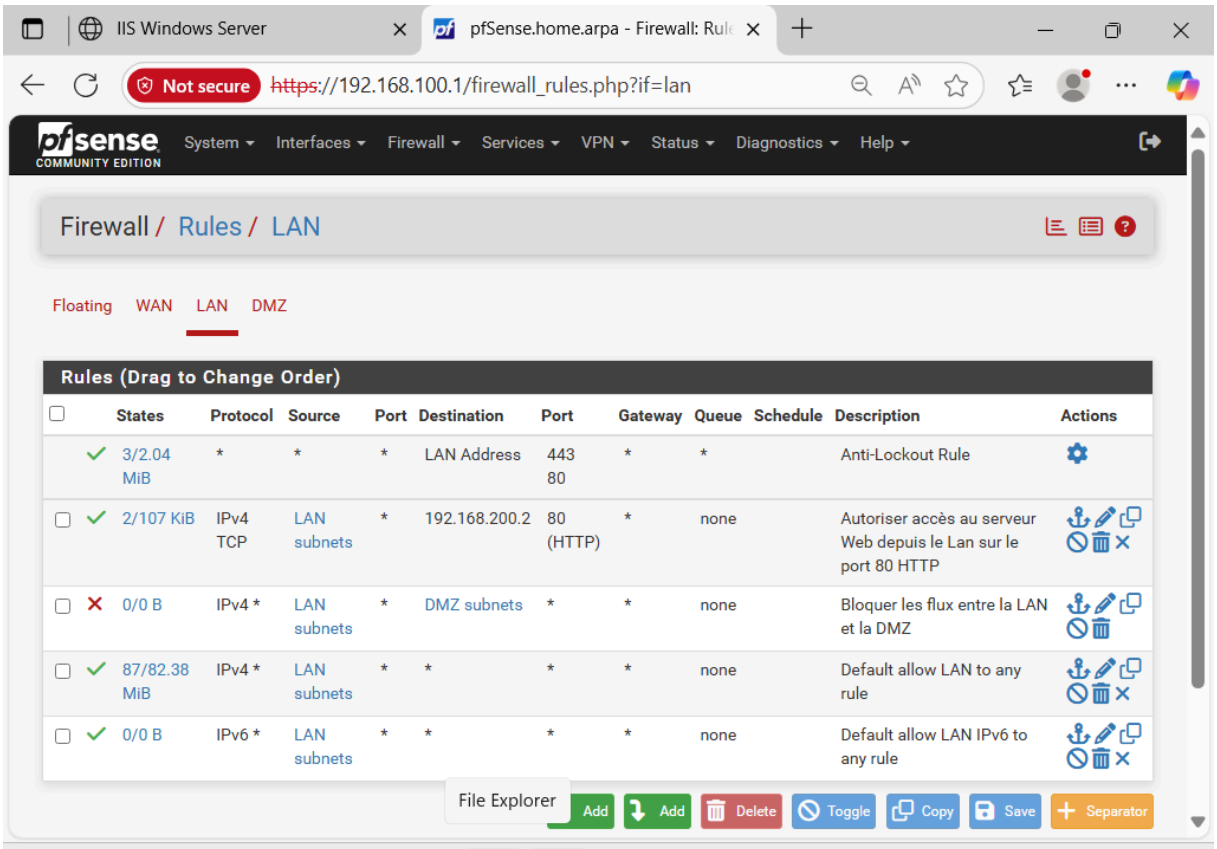


- Règles du Firewall DMZ

Interface LAN

Sur l'interface **LAN**, pfSense installe automatiquement une **Anti-Lockout Rule** qui autorise le trafic vers son adresse d'administration (ports 80 et 443) afin d'éviter que je ne sois bloqué hors de l'interface web. Juste en dessous, j'ai ajouté une règle très ciblée pour autoriser les clients du LAN à se connecter **uniquement sur le port HTTP (80)** vers l'adresse IP de mon serveur web en DMZ (192.168.200.2). Cette règle garantit que les utilisateurs internes ne peuvent accéder qu'au service web nécessaire, sans possibilité de connexions sur d'autres ports.

Pour appliquer le principe du moindre privilège, j'ai ensuite créé une règle bloquant **tout le trafic** LAN → DMZ, quel que soit le protocole. Cette règle se place juste après l'autorisation HTTP pour s'assurer que seul ce dernier passe. Enfin, j'ai conservé la règle par défaut **Allow LAN to any** pour permettre aux postes internes d'accéder librement à Internet et aux autres réseaux, sauf si une règle plus spécifique vient restreindre ce trafic.



- Règles du Firewall LAN

Grâce à cette organisation, je m'assure que :

- la **DMZ** reste isolée du **LAN** et ne peut initier que des connexions DNS, HTTP et HTTPS vers l'extérieur,
- le **LAN** ne peut accéder qu'au **service web** exposé en DMZ, et pas à d'autres ressources,
- je préserve l'accès à l'interface pfSense tout au long de ma configuration.

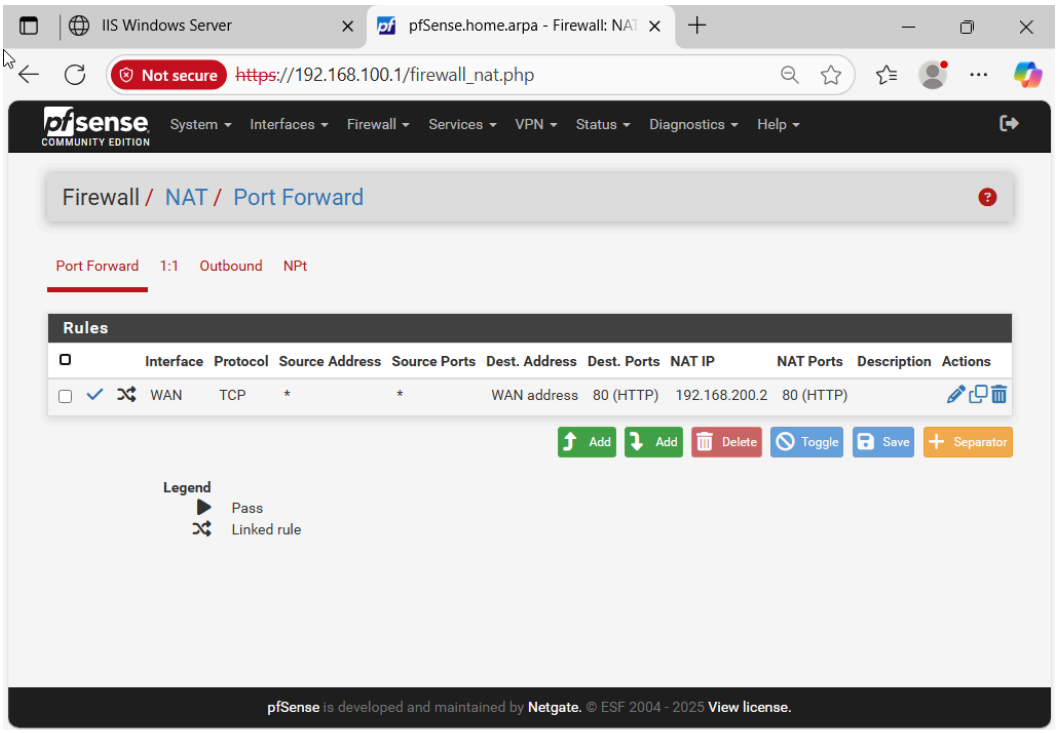
VIII. Configurer pfSense : règle de NAT pour le serveur Web

Pour permettre à un utilisateur depuis **Internet** (l'interface WAN) d'accéder à mon **serveur Web** hébergé en DMZ, je configure une règle de **port forwarding (NAT)**.

1. Création de la règle de NAT

Dans pfSense, je vais dans Firewall > NAT > Port Forward, puis je clique sur Add pour définir une nouvelle règle :

1. Interface : WAN
2. Protocol : TCP
3. Destination : WAN address (l'adresse IP publique de mon pfSense)
4. Destination port range : HTTP (80)
5. Redirect target IP : `192.168.200.2` (mon serveur Web en DMZ)
6. Redirect target port : HTTP (80)
7. Description : `NAT HTTP vers serveur Web DMZ`



- *Règle NAT*

Après avoir cliqué sur Save puis Apply Changes, pfSense est censé rediriger tout trafic TCP arrivant sur le port 80 de son WAN vers le serveur DMZ.

2. Test initial et particularité du mode Bridge

Je teste d'abord depuis ma machine physique (connectée en « WAN »), en saisissant dans un navigateur .

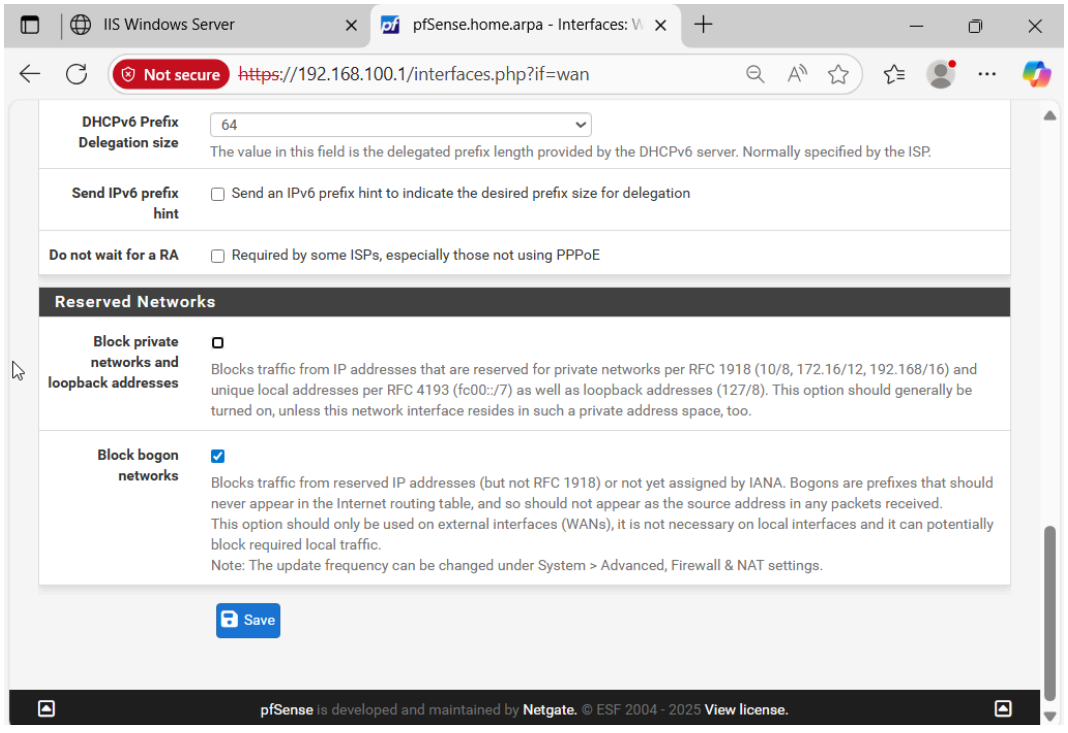
Le site ne se charge pas. Sur mon lab en mode Bridge, pfSense bloque par défaut les adresses privées (RFC 1918) arrivant sur son interface WAN, via l'option Block private network and loopback addresses.

3. Désactivation de l'option « Block private networks »

Pour autoriser le test depuis mon réseau local (qui utilise des adresses privées), je vais dans System > Advanced > Firewall & NAT et je désactive :

Block private network and loopback addresses

Cette option empêche normalement qu'un paquet dont l'IP source est en 192.168.x.x n'arrive sur mon WAN.

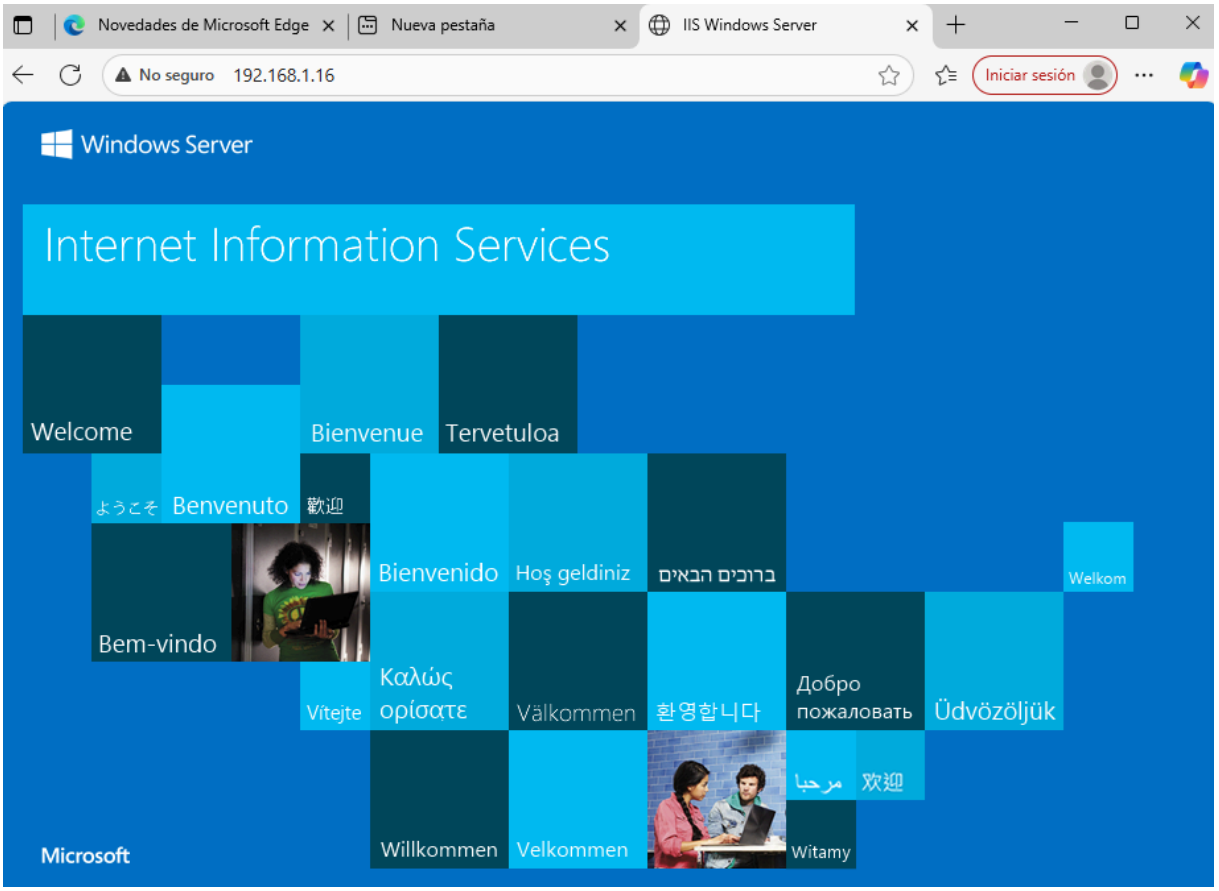


- *Désactivation de "Block private network and loopback addresses"*

Je sauvegarde et applique les modifications.

4. Résultat final

De retour sur ma machine physique, je rafraîchis l'URL :



Cette fois, la page IIS s'affiche correctement : le trafic WAN → DMZ est bien redirigé via la règle de NAT.

Bilan : grâce à cette configuration, mon serveur web en DMZ est accessible depuis l'extérieur tout en restant isolé du LAN interne, et j'ai contourné la protection anti-RFC 1918 du mode Bridge pour mes tests.

IX. Conclusion

Mission accomplie ! J'ai mis en place **un pare-feu pfSense** structuré autour de trois zones réseau :

- Une interface **WAN** simulant Internet,
- Une interface **LAN** pour mes postes internes,
- Une **DMZ** hébergeant un serveur web Windows Server 2025 sous IIS.

J'ai configuré les interfaces réseau, défini des règles de firewall précises (bloquant tout flux LAN→DMZ sauf HTTP, et limitant la DMZ à DNS/HTTP/HTTPS vers Internet), et créé une règle NAT pour rendre le site accessible depuis l'extérieur. Grâce à cette architecture et à ces contrôles, mon serveur web est :

1. Accessible depuis le LAN uniquement sur le port 80,
2. Accessible depuis Internet via la règle de port forwarding sur le WAN,
3. Complètement isolé du LAN sur les autres protocoles.

Perspectives d'évolution

Pour aller plus loin, je pourrais :

- Publier mon site via un reverse proxy (Package HAProxy sur pfSense) pour renforcer la sécurité et gérer la terminaison TLS,
- Mettre en place un certificat Let's Encrypt automatisé (via ACME),
- Ajouter un IDS/IPS (Snort ou Suricata) pour surveiller les intrusions,
- Déployer un honeypot en DMZ pour analyser les attaques réelles,
- Configurer des VPN (OpenVPN ou IPsec) pour des accès sécurisés à distance.

Ce lab virtuel constitue une base solide pour expérimenter et approfondir les notions de segmentation réseau, filtrage, NAT, et services sécurisés.