Mise en Place et Réglages PfSense

BTS S.I.O. option S.I.S.R – 2025 - 2026

Mr Michele Mastrogiacomo

Description de PfSense

PfSense, basé sur un fork de m0n0wall réalisé en 2004 par Chris Buechler et Scott Ullrich, est un système d'exploitation open source dans les fonctions de pare-feu et routeur. Il est utilisé bien à domicile que dans des environnements professionnels.

PfSense peut fonctionner sur du matériel de serveur ou domestique sans demander beaucoup de ressource ni de matériel puissant, une CPU de 1GHZ et Ram de 1GB c'est suffisant.

pfSense permet de : filtrer du trafic entrant et sortant, mettre en place un VPN, NAT, possibilité d'un DHCP, DNS, Surveiller et analyser le trafic réseau, bloquer de contenu ou sites.

Utilisation de PfSense dans ce TP

Dans le cadre de mon stage j'ai proposé ce pare-feu qui fait partie de l'infrastructure réseau.

Le réseau, dans le cas de ce travaux pratique, est organisé en plusieurs bâtiments (informatique, ateliers, classes et administratif) et intègre différents services tels qu'un serveur Active Directory, un serveur de fichiers ainsi qu'un système de sauvegarde NAS. Une zone démilitarisée (DMZ) est également mise en place pour héberger un serveur web accessible depuis l'extérieur.

Les objectifs du projet :

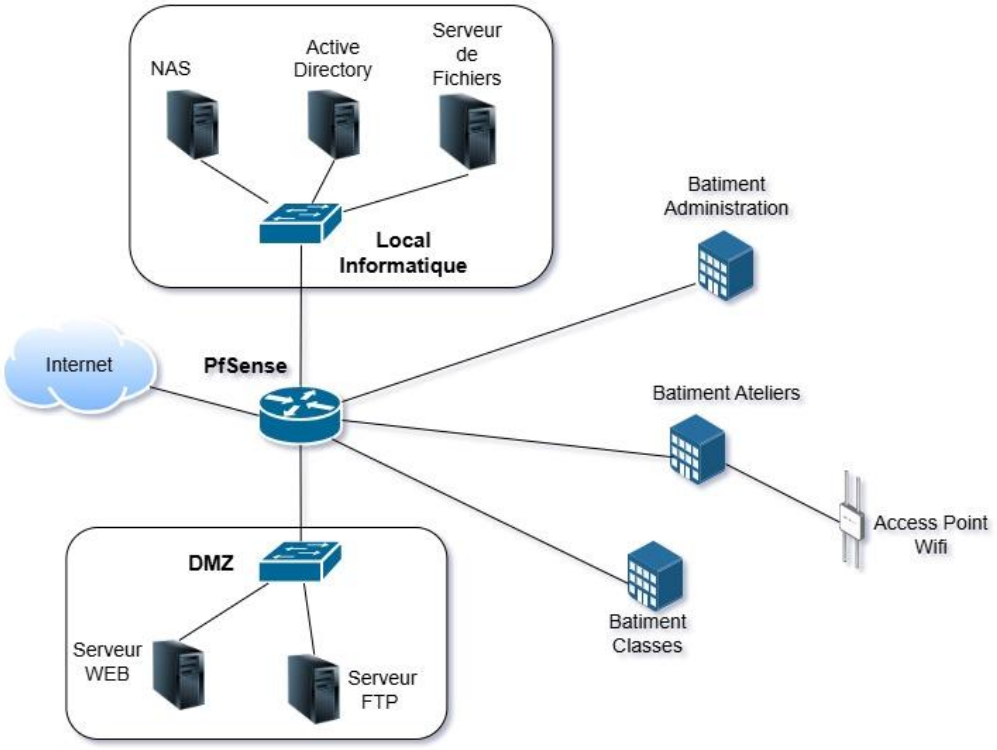
- Mettre en place une segmentation du réseau (LAN, DMZ, bâtiments)
- Sécuriser les communications
- Déployer les services essentiels (Active Directory, fichiers, sauvegarde)
- Contrôler les flux réseau grâce aux règles de filtrage et au NAT
- Tester et valider le bon fonctionnement

Présentation de l'environnement

L'architecture réseau proposée est basée sur un environnement scolaire réparti en plusieurs bâtiments : Bâtiment Informatique, Bat. Ateliers, Bat. Classes, Bat. Administratif

Chaque bâtiment correspond à un réseau distinct afin de garantir une segmentation logique

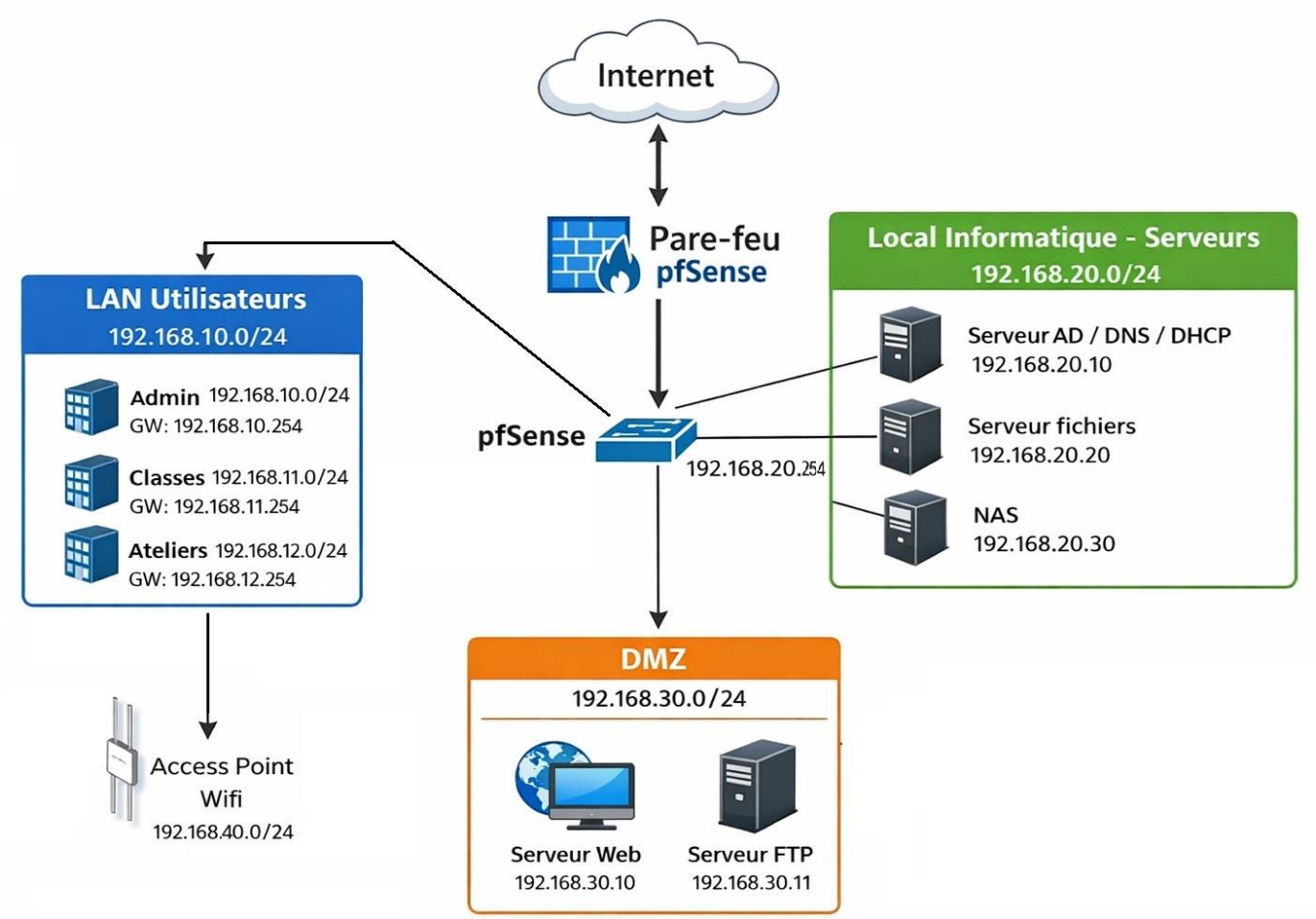
Image1 - Schéma réseau dont pfSense est la principal sécurité entre internet et le LAN



Plan d'adressage IP

J'ai créé un plan d'adressage pour organiser les différents réseaux, qui permet de faciliter la gestion, d'améliorer la sécurité et de simplifier la mise en place des règles de filtrage.

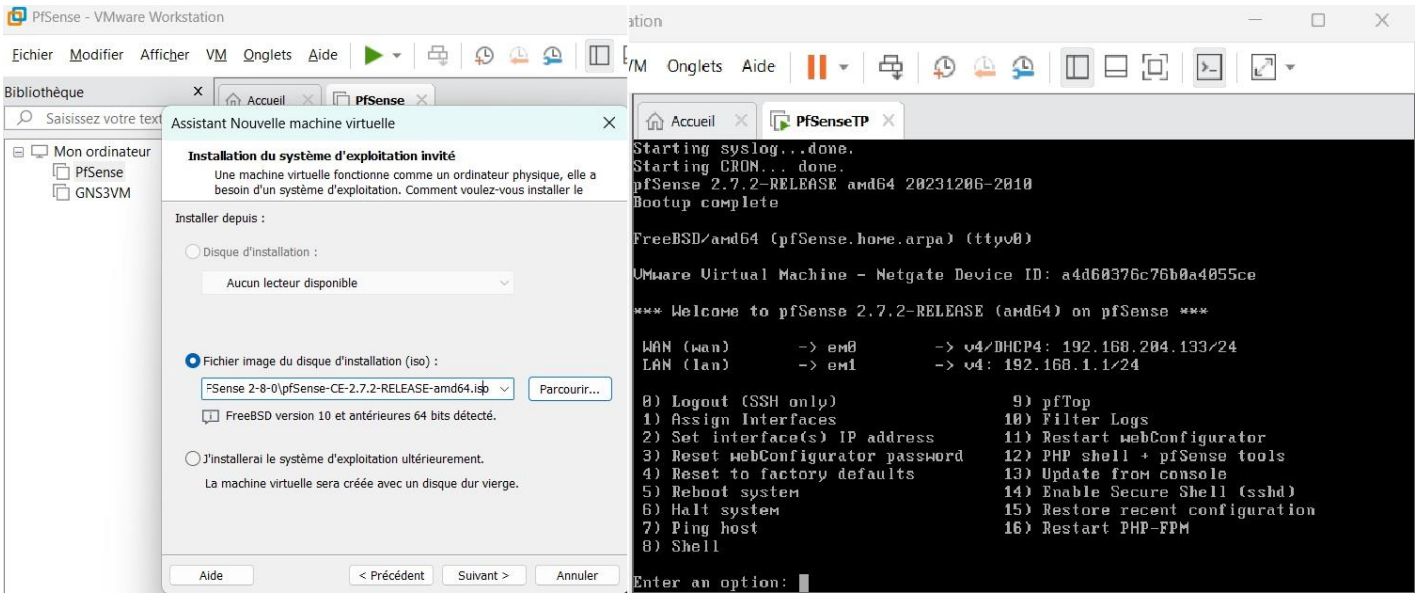
Image2 – Plan d'adressage a insérer en pfSense



Installation de pfSense

L'installation de pfSense est simple, j'ai d'abord crée une machine virtuelle sous VMware qui ensuite est lié au simulateur de réseau GNS3. Avec ou sans machine virtuelle l'installation est identique en partant du file image d'installation.

Image2 – Creation machine virtuelle et fin d'installation pfsense



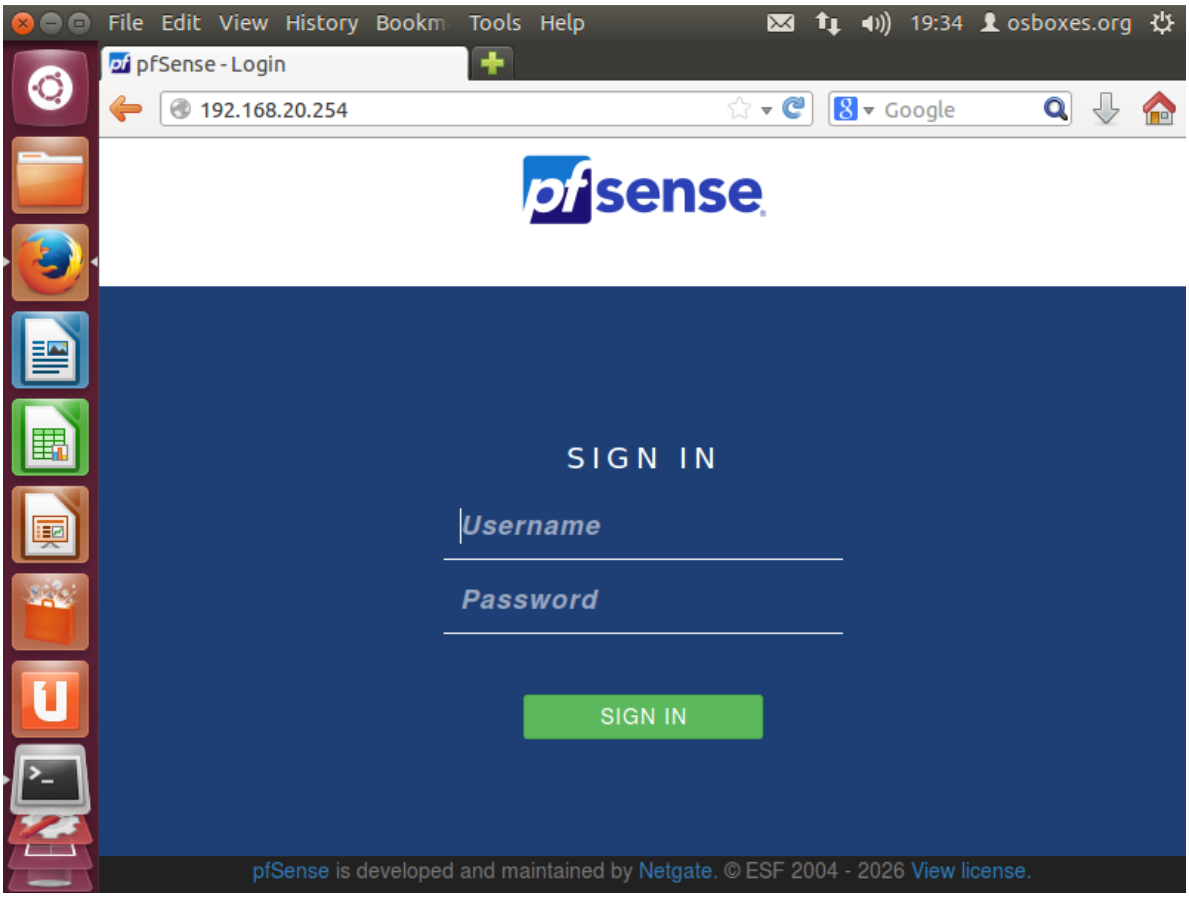
Accès à l'interface web et configuration lan

J'ai effectué la première configuration en donnant l'adresse 192.168.20.254 au router pfSense et j'ai dit oui pour y avoir accès sous http(travers un browser)

Image3 – Configuration IP et accès Web Pfsense

```
> 192.168.20.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.20.2
Enter the end address of the IPv4 client address range: 192.168.20.253
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
```

Image4 – Connexion PfSense depuis un Browser



Segmentation du réseau

Chaque bâtiment (informatique, ateliers, classes, administratif) dispose de son propre réseau.

Cette segmentation permet de limiter les communications entre les différents services merci au réglages et de réduire les risques en cas d'incident.

Chaque réseau est associé à une interface sur le pare-feu pfSense avec une adresse IP spécifique, jouant le rôle de passerelle.

Création des réseaux / VLAN

Je créer les interfaces pour le diffèrent réseau ceci est possible a faire travers le terminal de PfSense (1. Assigner les Interface 2. Assigner les adresse IP) ou en se connectant travers le l'interface web

Image 5 – Assignation des Interface sur PfSense travers le terminal

```
Enter an option: 1

Valid interfaces are:

em0     00:0c:29:a9:46:c5   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em1     00:0c:29:a9:46:cf   (up) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em2     00:0c:29:a9:46:01 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em3     00:0c:29:a9:46:f7 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em4     00:0c:29:a9:46:e3 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em5     00:0c:29:a9:46:ed (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)
em6     00:0c:29:a9:46:d9 (down) Intel(R) Legacy PRO/1000 MT 82545EM (Copper)

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y|n]? n

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 em3 em4 em5 em6 or a): em0
```

Image 6 – Assignation des Adresse IP travers l'interface web

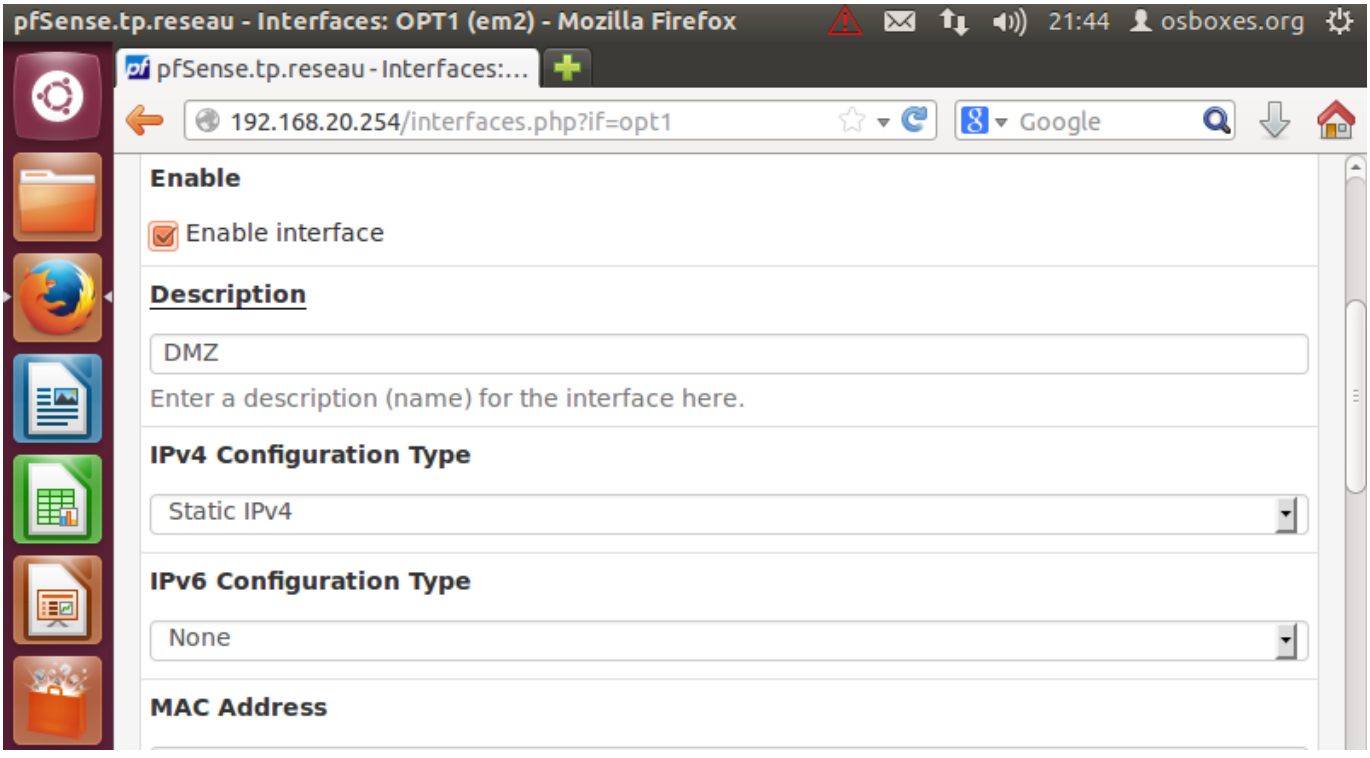
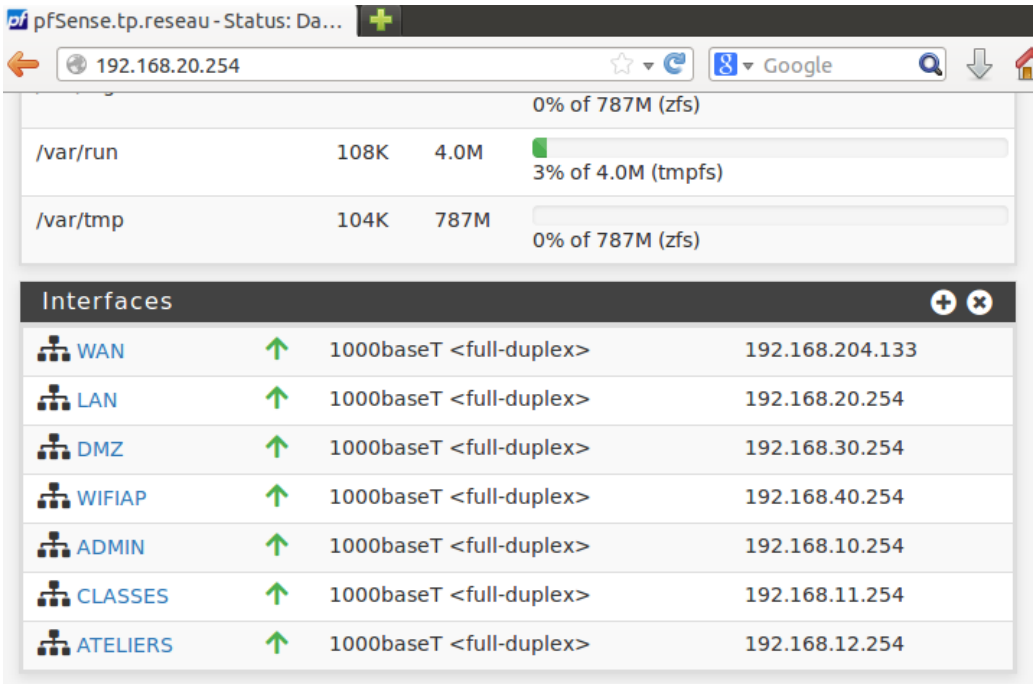


Image 7 – Liste d'adressage final dans pfSense



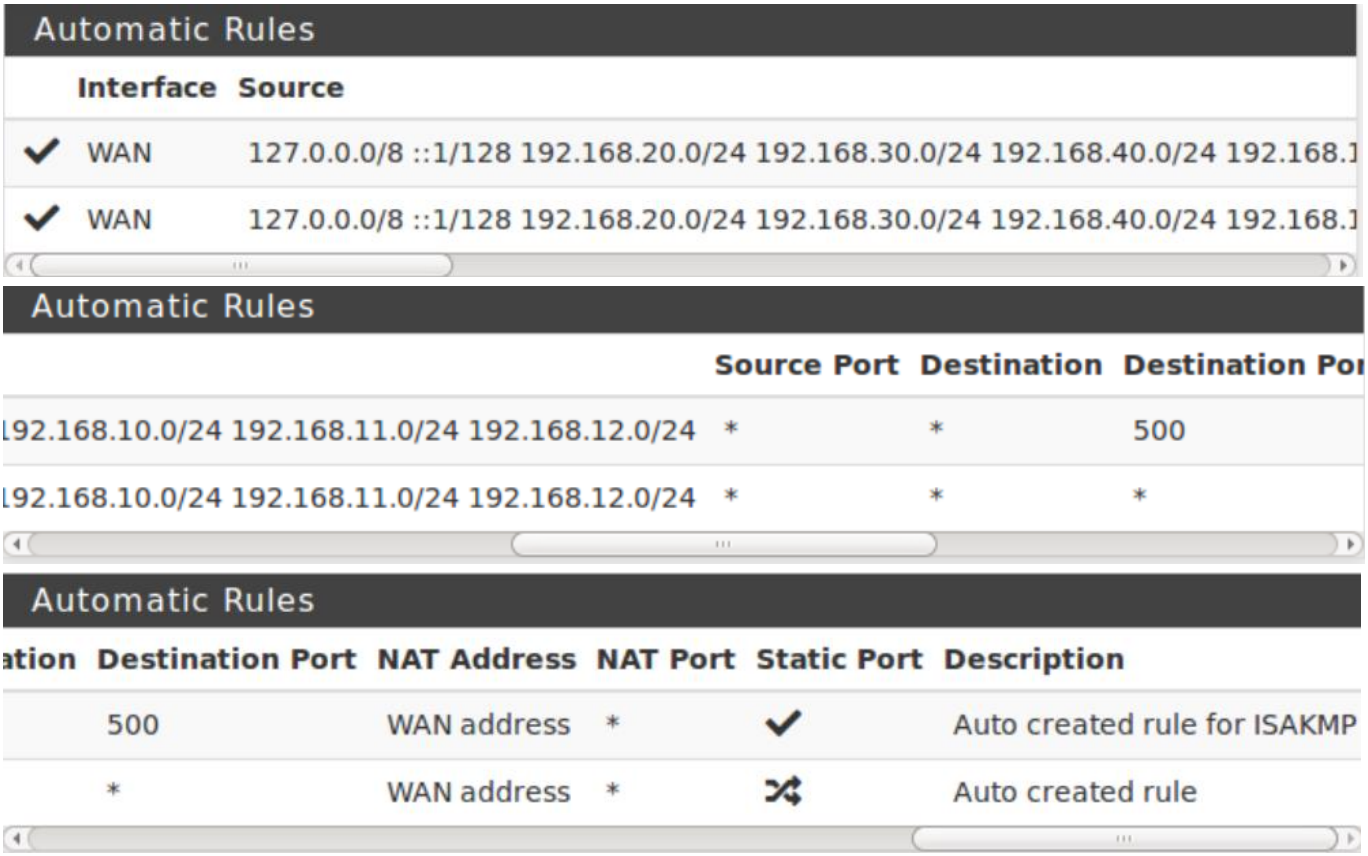
Mise en place du NAT

La traduction d'adresses (NAT) a été configurée afin de permettre aux machines du réseau interne d'accéder à Internet et des règles de redirection de ports pour rendre accessible le serveur en dmz depuis internet. Donc j'ai configuré:

NAT sortant **Outbound mode** (LAN → Internet) qui permet aux utilisateurs d'aller sur Internet

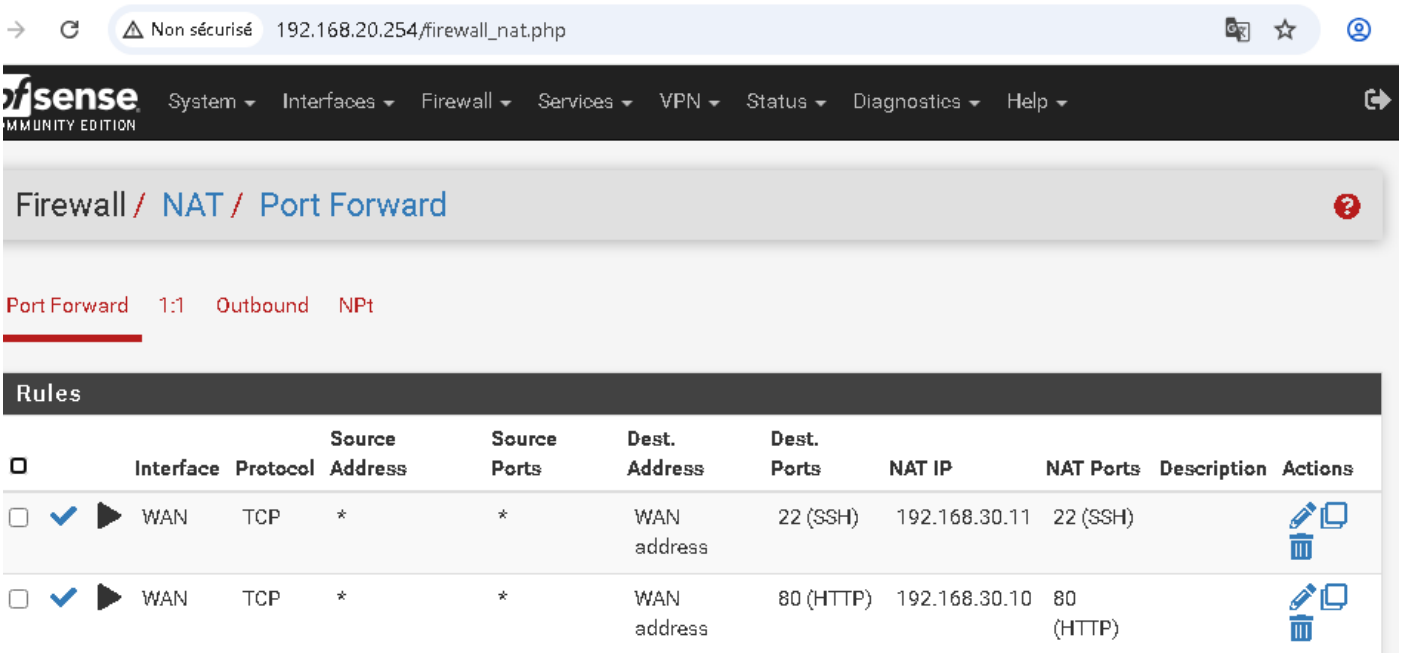
Ce réglage est mise sur automatique j'ai appliqué la règle et vérifié que tout était écrit.

Image 8 – Règle NAT Outbound de connexion Internet pour le reseau



Ensuite la configuration pour le :
NAT entrant (Port Forwarding) → DMZ qui permet d'accéder au serveur web depuis Internet
Les requêtes arrivant sur le port 80 de l'interface WAN sont redirigées vers le serveur web situé dans la DMZ. La même règle est ajouté pour avoir accès au serveur SFTP

Image 9 – Règle NAT Port Forwarding Accès au Serveur web et sftp depuis Internet



Configuration des règles Pare-feu

La configuration des règles de filtrage constitue un élément essentiel de la sécurisation du réseau, permettant de contrôler précisément les échanges entre les différentes zones.

Un alias est un objet qui regroupe plusieurs éléments, un alias de ports a été créé afin d'autoriser en une seule règle les flux nécessaires depuis la DMZ vers Internet (HTTP, HTTPS, NTP, SSH). Cela évite de multiplier les règles individuelles pour chaque port, ce qui rend la configuration plus lisible, plus facile à maintenir et moins sujette aux erreurs. En cas de modification (ajout ou suppression d'un port), il suffit de mettre à jour l'alias sans avoir à modifier toutes les règles associées. La règle autorisant les requêtes DNS depuis la DMZ vers le serveur Active Directory permet aux serveurs de la DMZ de résoudre les noms de domaine en utilisant le DNS interne, tout en maintenant l'isolation du réseau interne grâce à un accès strictement limité au port 53.

Les règles suivantes ont été définies :

- Autoriser les machines du LAN à accéder à Internet
- Une autorisation requêtes DNS depuis la DMZ vers le serveur Active Directory
- Bloquer les communications de la DMZ vers le LAN afin de protéger le réseau interne
- Autoriser les connexion interne ver le Serveur WEB et FTP travers internet

Image 10 – Créations des Aliases Port

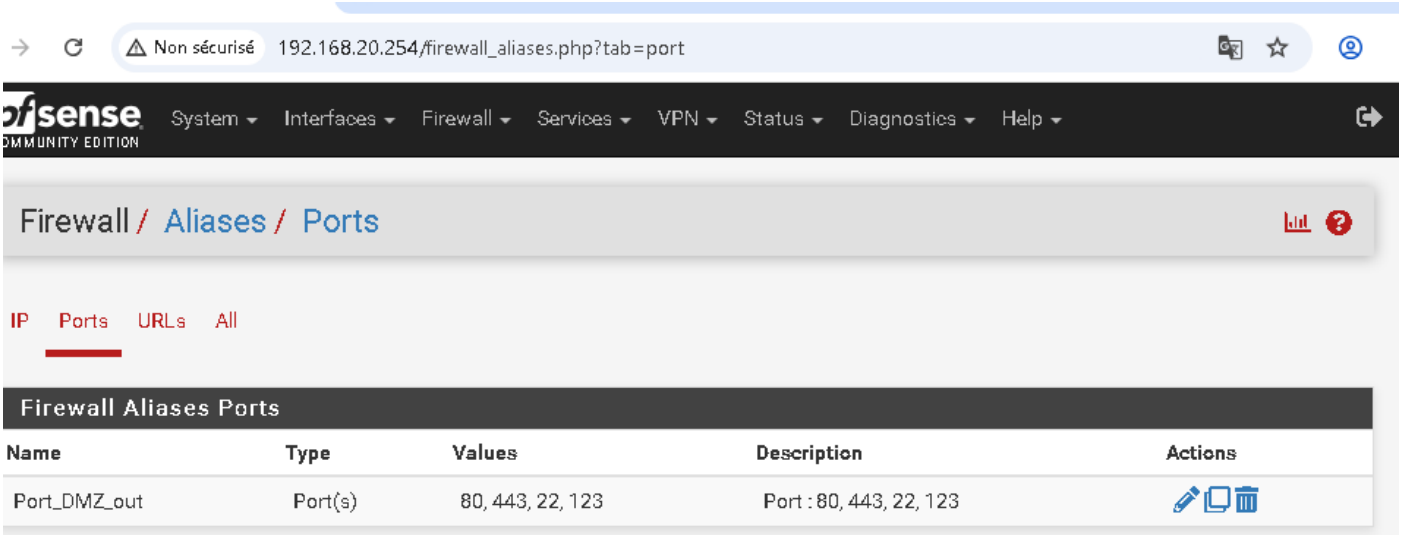


Image 11 – Créations des Aliases saufWAN

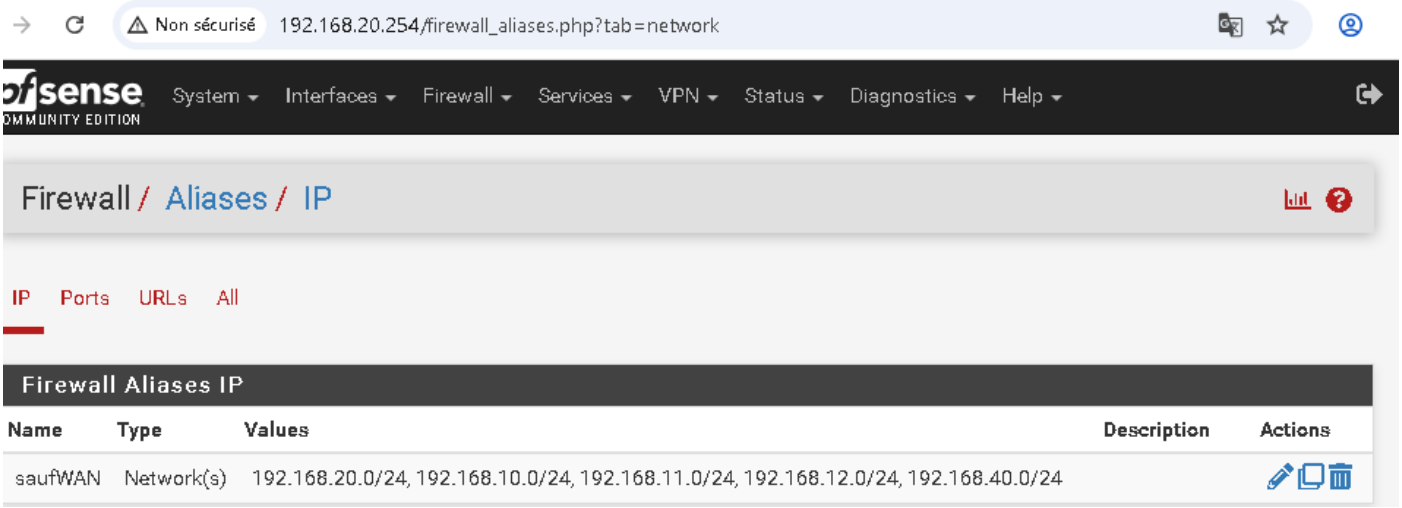


Image 12 – Blocages de connexion DMZ vers LAN sauf pour Internet port HTTP DNS SFTP

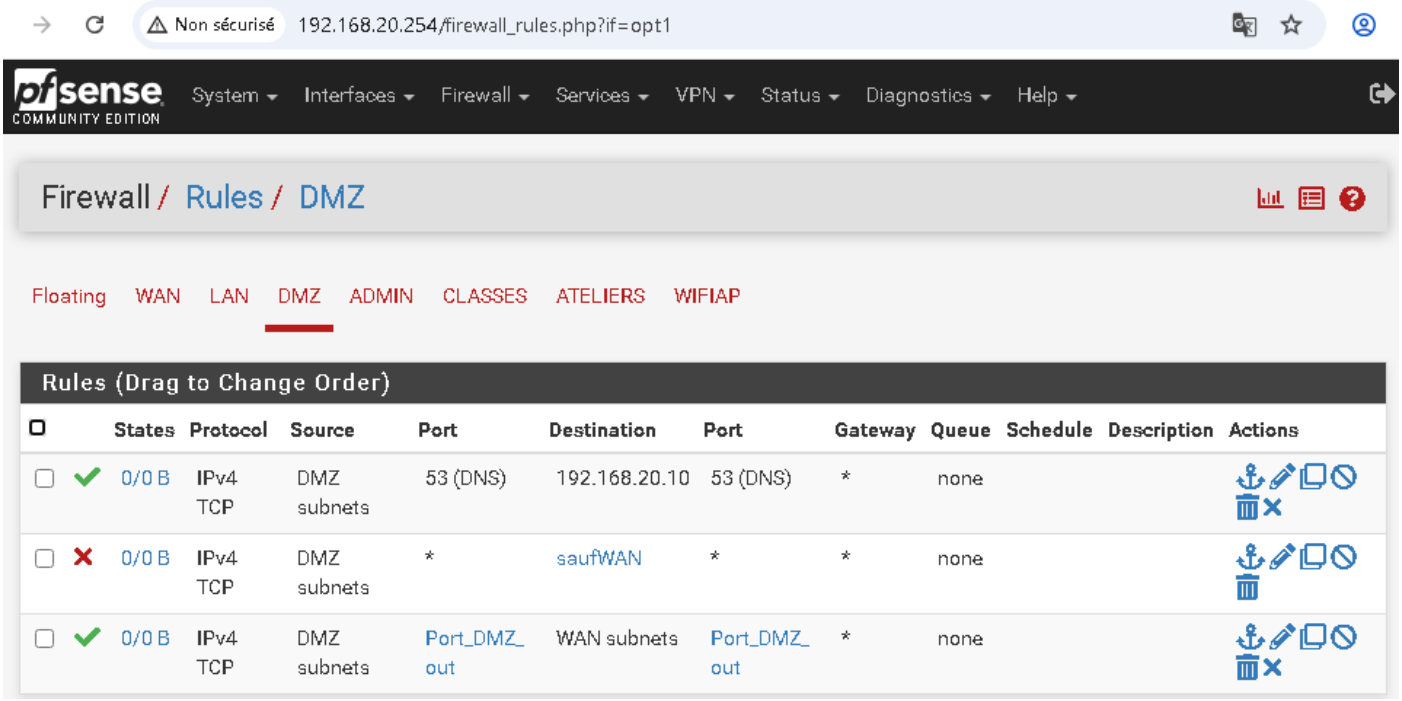
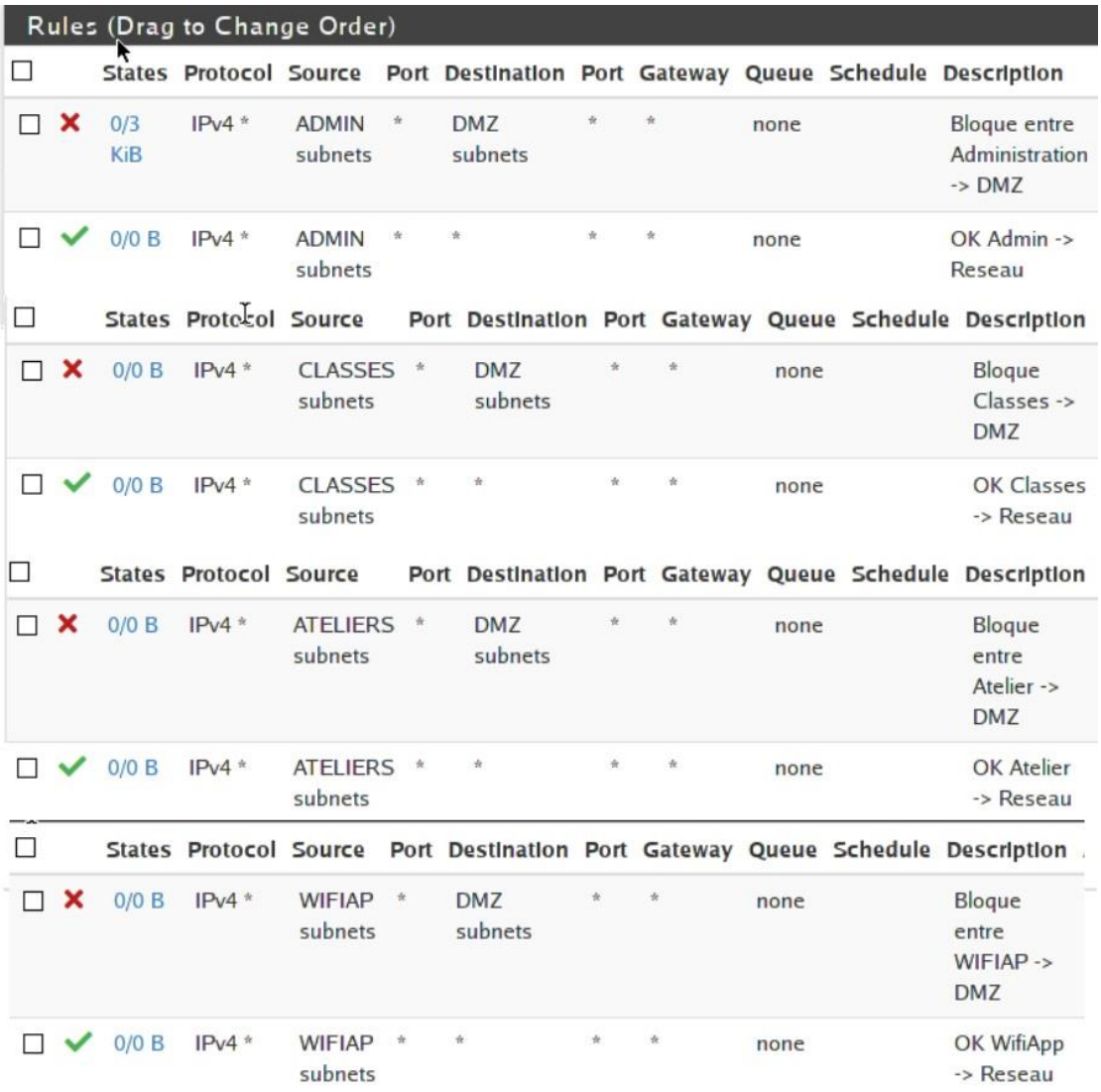


Image 13 – Blocage communication du LAN ver le DMZ et Autorisation du LAN au réseau interne

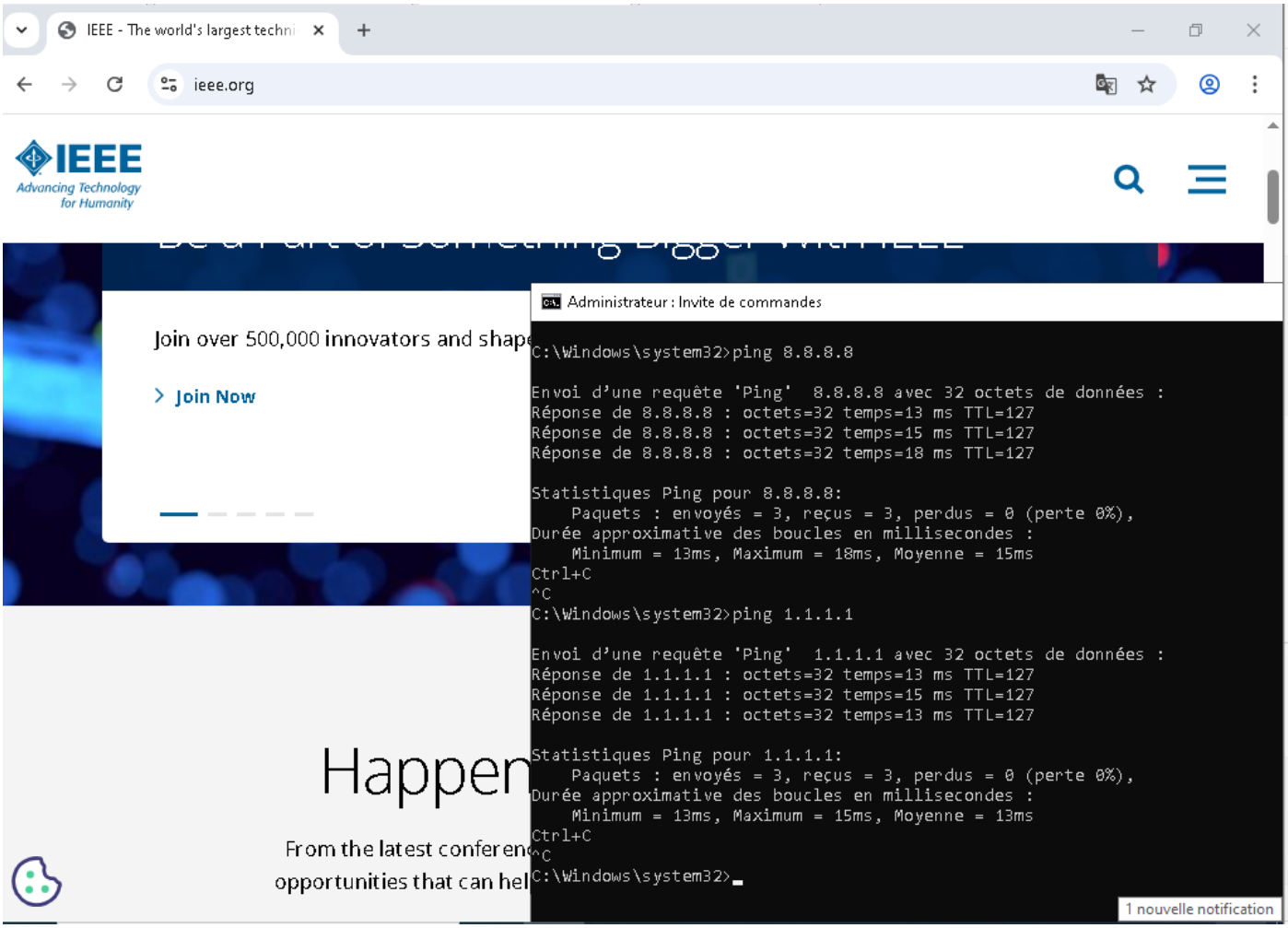


Tests de fonctionnement de règles et validation

Test de communication LAN → Internet

Le ping vers une IP publique ainsi que l'ouverture d'un site web confirment que le NAT et la configuration WAN fonctionnent correctement.

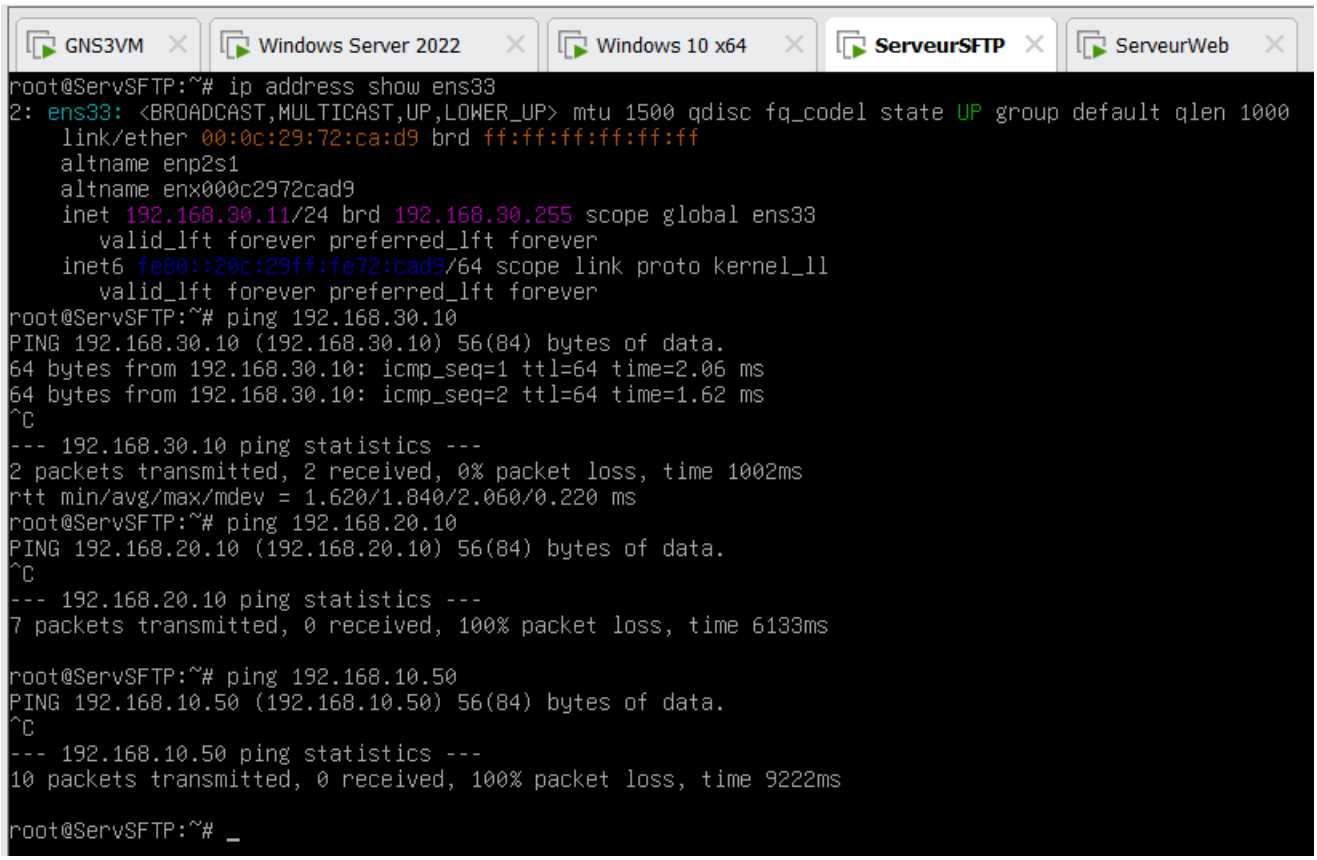
Image 14 – Ping , Page ouverte depuis un poste en LAN



Test d'isolation DMZ

L'isolation de la DMZ a été testée pour vérifier que les machines de cette zone ne peuvent pas accéder directement au LAN et vice-versa que le LAN ne peut pas se connecter directement au DMZ

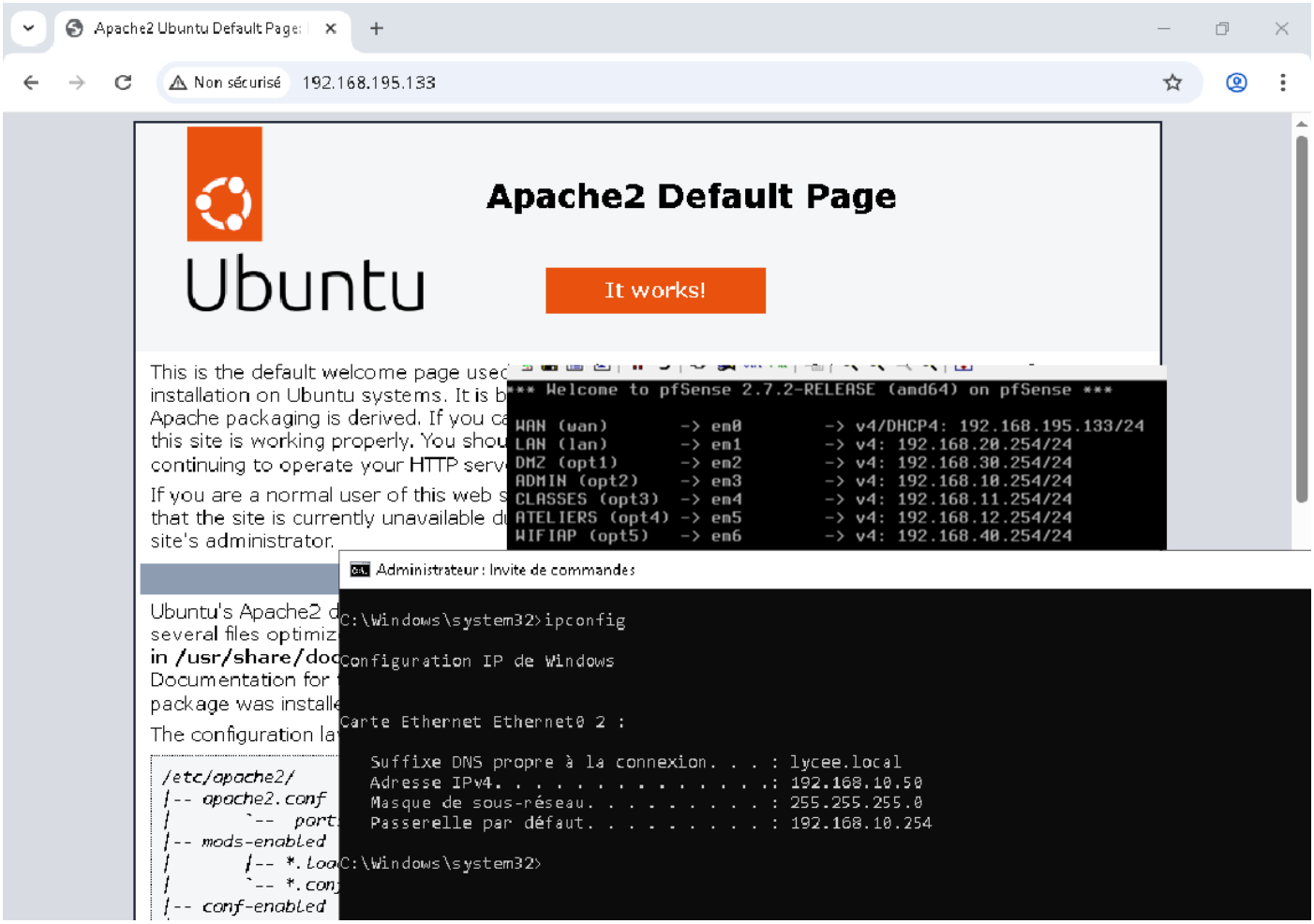
Image 15 – Ping du poste en DMZ vers LAN



Test d'accès aux Serveur WEB et FTP

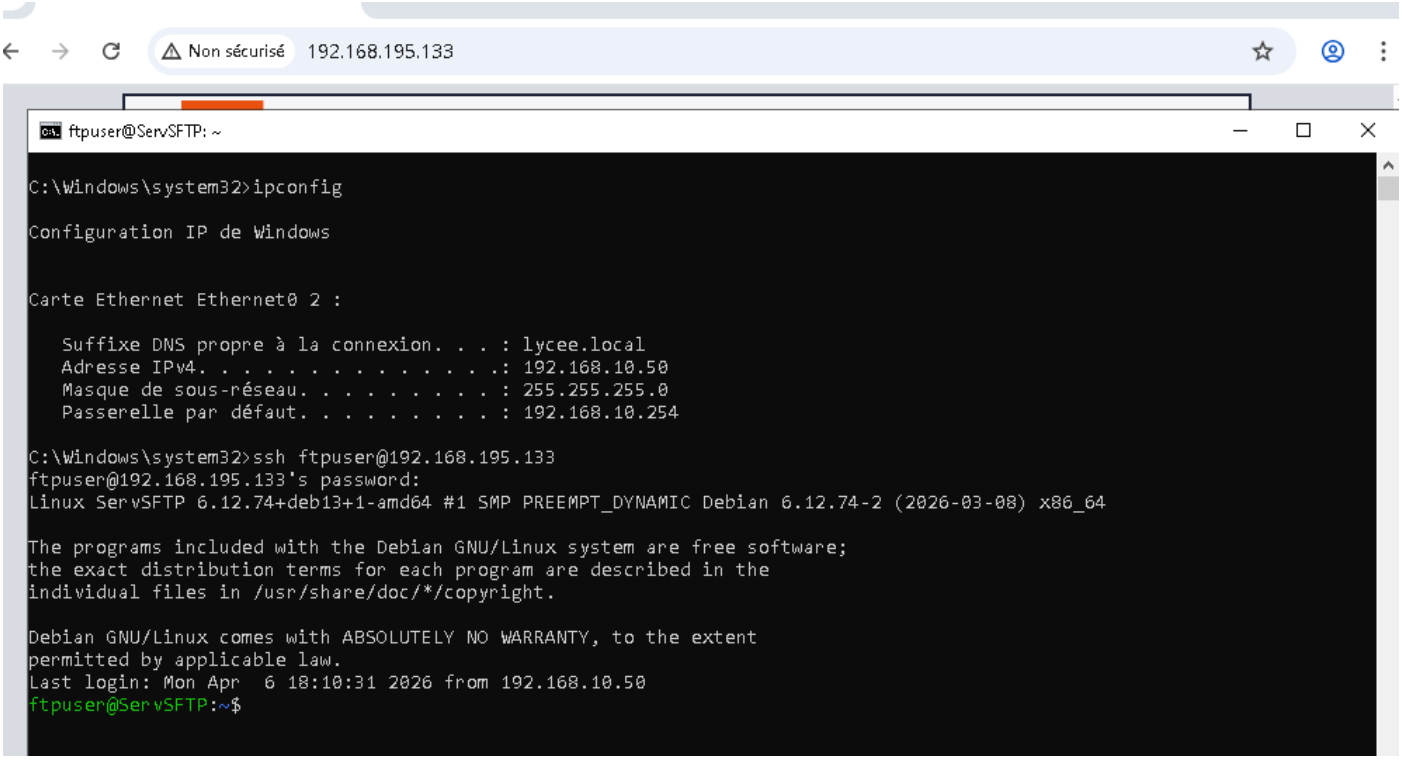
L'accès au serveur web depuis l'extérieur a été testé via navigateur Internet. La redirection NAT fonctionne correctement et permet la communication sécurisée entre le client Internet et le serveur situé dans la DMZ.

Image 16 - Navigateur depuis le WAN



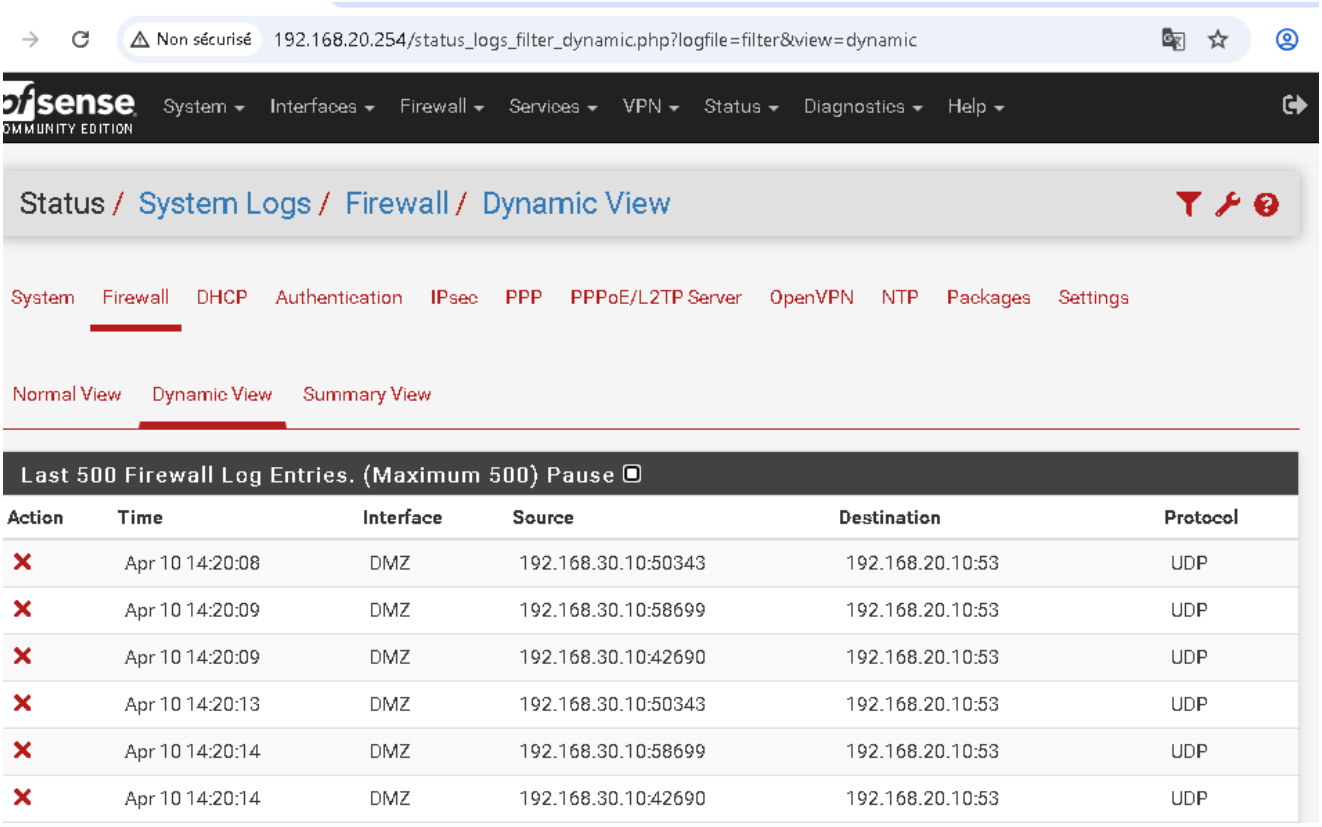
Le serveur FTP est accessible depuis Internet via le port 21 grâce à la redirection NAT correspondante.

Image 17 - connexion SFTP depuis une machine externe



Vérification des règles de firewall

Les logs du pare-feu ont été vérifiés afin de confirmer que seules les communications autorisées sont passées et que toutes les règles définies (LAN → Internet, DMZ isolée, accès NAT) sont respectées.



Action	Time	Interface	Source	Destination	Protocol
✕	Apr 10 14:20:08	DMZ	192.168.30.10:50343	192.168.20.10:53	UDP
✕	Apr 10 14:20:09	DMZ	192.168.30.10:58699	192.168.20.10:53	UDP
✕	Apr 10 14:20:09	DMZ	192.168.30.10:42690	192.168.20.10:53	UDP
✕	Apr 10 14:20:13	DMZ	192.168.30.10:50343	192.168.20.10:53	UDP
✕	Apr 10 14:20:14	DMZ	192.168.30.10:58699	192.168.20.10:53	UDP
✕	Apr 10 14:20:14	DMZ	192.168.30.10:42690	192.168.20.10:53	UDP