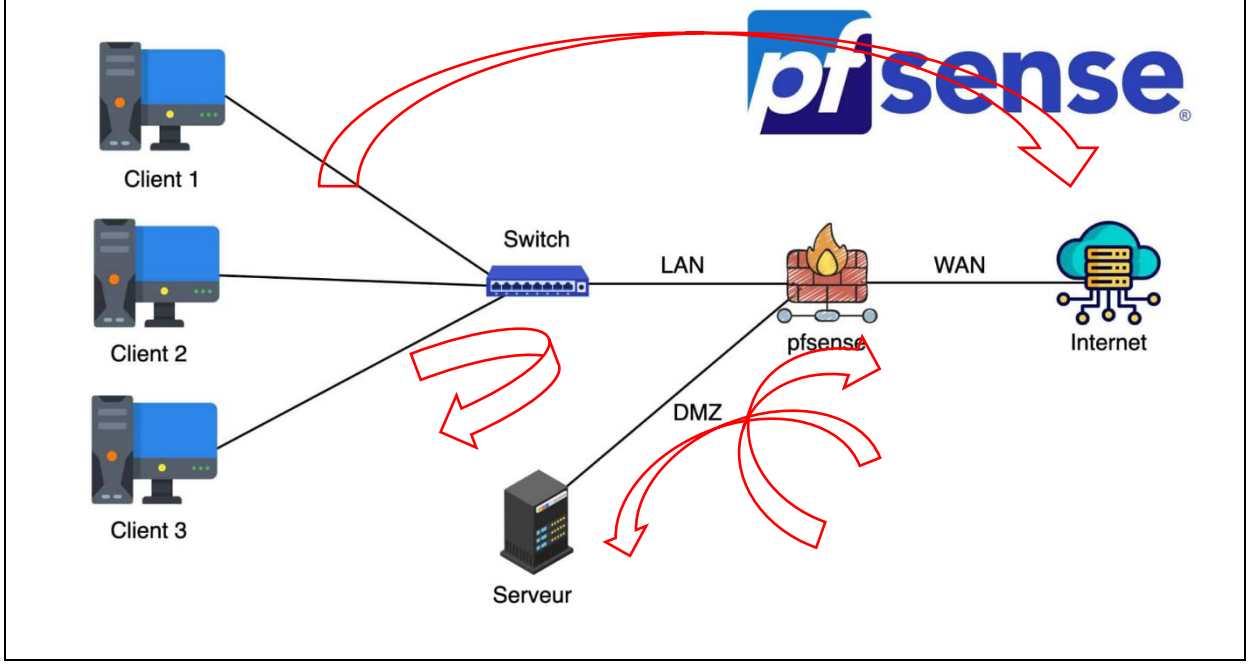
Configuration du pare-feu pfSense et gestion des règles de filtrage



1. Introduction

Dans ce tutoriel, nous allons configurer les **règles de pare-feu** sur pfSense afin de permettre et de contrôler la communication entre les différents réseaux de notre infrastructure. Cette configuration vise à assurer la **sécurité et l'isolation des flux** entre la DMZ, le réseau interne (LAN) et Internet (WAN).

Définition de quelques notions :

Qu'est-ce que pfSense ?

pfSense est un **pare-feu open-source et une solution de routage avancée** basée sur FreeBSD. Il permet de sécuriser un réseau en contrôlant le trafic entrant et sortant à travers des règles personnalisables. Il est couramment utilisé pour gérer les réseaux d'entreprise grâce à ses fonctionnalités telles que le filtrage de paquets, le VPN, la gestion des VLANs et la détection d'intrusions.

Qu'est-ce qu'une DMZ ?

Une **DMZ (Demilitarized Zone)** est un sous-réseau isolé du réseau interne (LAN) et accessible depuis l'extérieur. Elle est utilisée pour héberger des serveurs accessibles publiquement (serveurs web, serveurs de messagerie, etc.) tout en protégeant le réseau interne contre les attaques potentielles. L'objectif principal de la DMZ est de minimiser les risques d'intrusion dans le LAN en maintenant une séparation stricte entre les zones sensibles et les services exposés.

Qu'est-ce qu'un LAN ?

Le **LAN (Local Area Network)** représente le réseau interne d'une organisation. Il est constitué des postes de travail, des imprimantes, des serveurs internes et d'autres équipements connectés. Contrairement à la DMZ, le LAN est destiné aux utilisateurs internes et est généralement protégé contre l'accès extérieur grâce à un pare-feu comme pfSense.

2. Objectifs

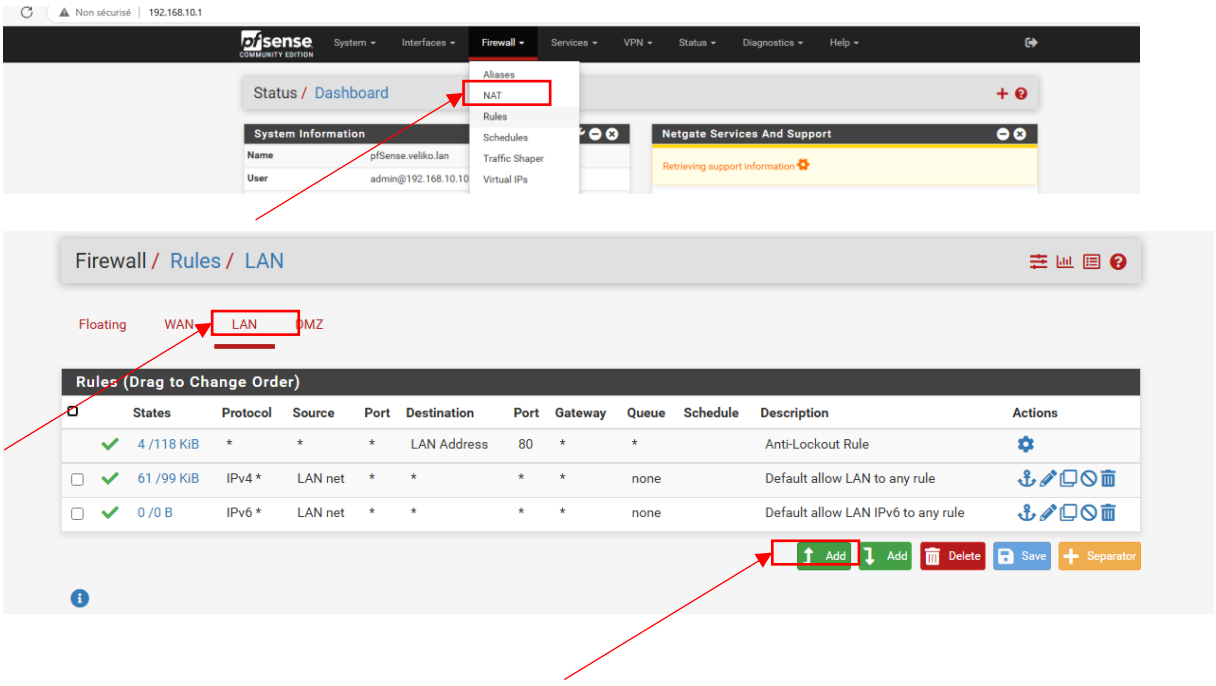
L'objectif principal est de définir des règles de filtrage pour :

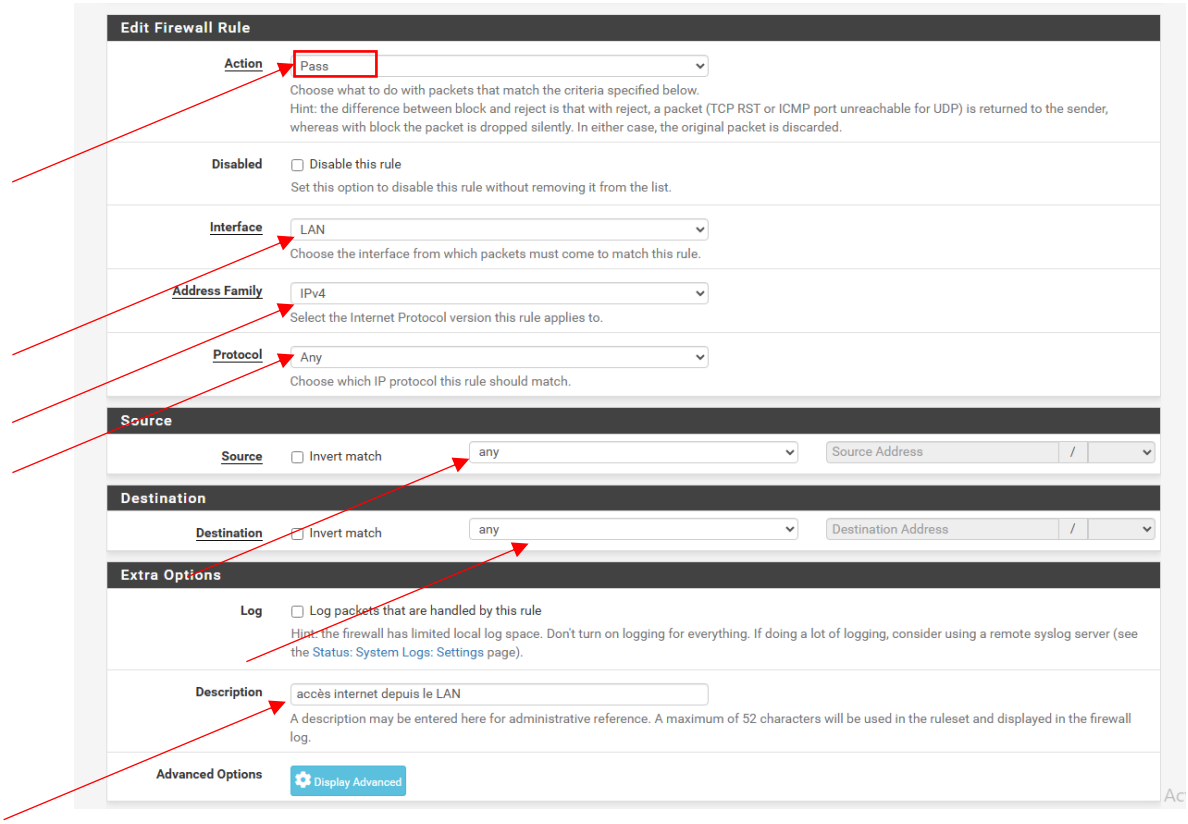
- **Autoriser l'accès à Internet depuis le LAN et la DMZ**
- **Bloquer l'accès direct de la DMZ vers le LAN**
- **Autoriser l'accès au serveur web situé en DMZ depuis le LAN**
- **Configurer le NAT pour permettre l'accès à un service depuis l'extérieur**

3. Configuration des règles de pare-feu

3.1 Autoriser le LAN à accéder à Internet

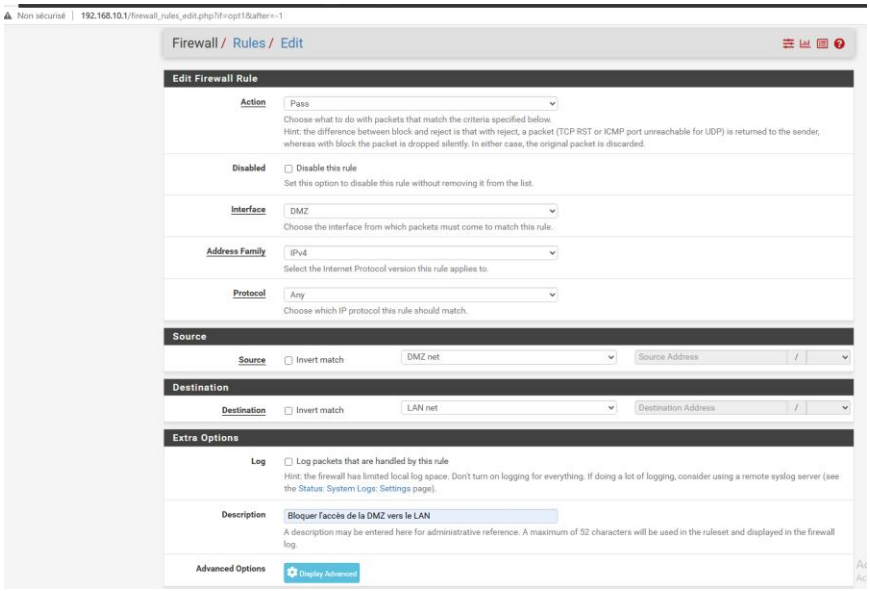
1. Connectez-vous à l'interface web de pfSense.
2. Accédez à **Firewall > Rules>LAN>Add** pour créer une nouvelle règle.
3. Configurez la règle comme suit :





3.2 Bloquer l'accès de la DMZ vers le LAN

1. Rendez-vous dans **Firewall > Rules**> **DMZ> Add** et créez une règle avec les paramètres suivants :
    - **Action** : Block
    - **Interface** : DMZ
    - **Protocol** : Any
    - **Source** : DMZ net
    - **Destination** : LAN net



2. Enregistrez la règle et appliquez les changements.

3.3Autoriser le LAN à accéder au serveur web en DMZ

4 Toujours dans **Firewall > Rules**, sélectionnez **LAN**>**Add** et configurez la règle comme suit :

4.2Action : Pass

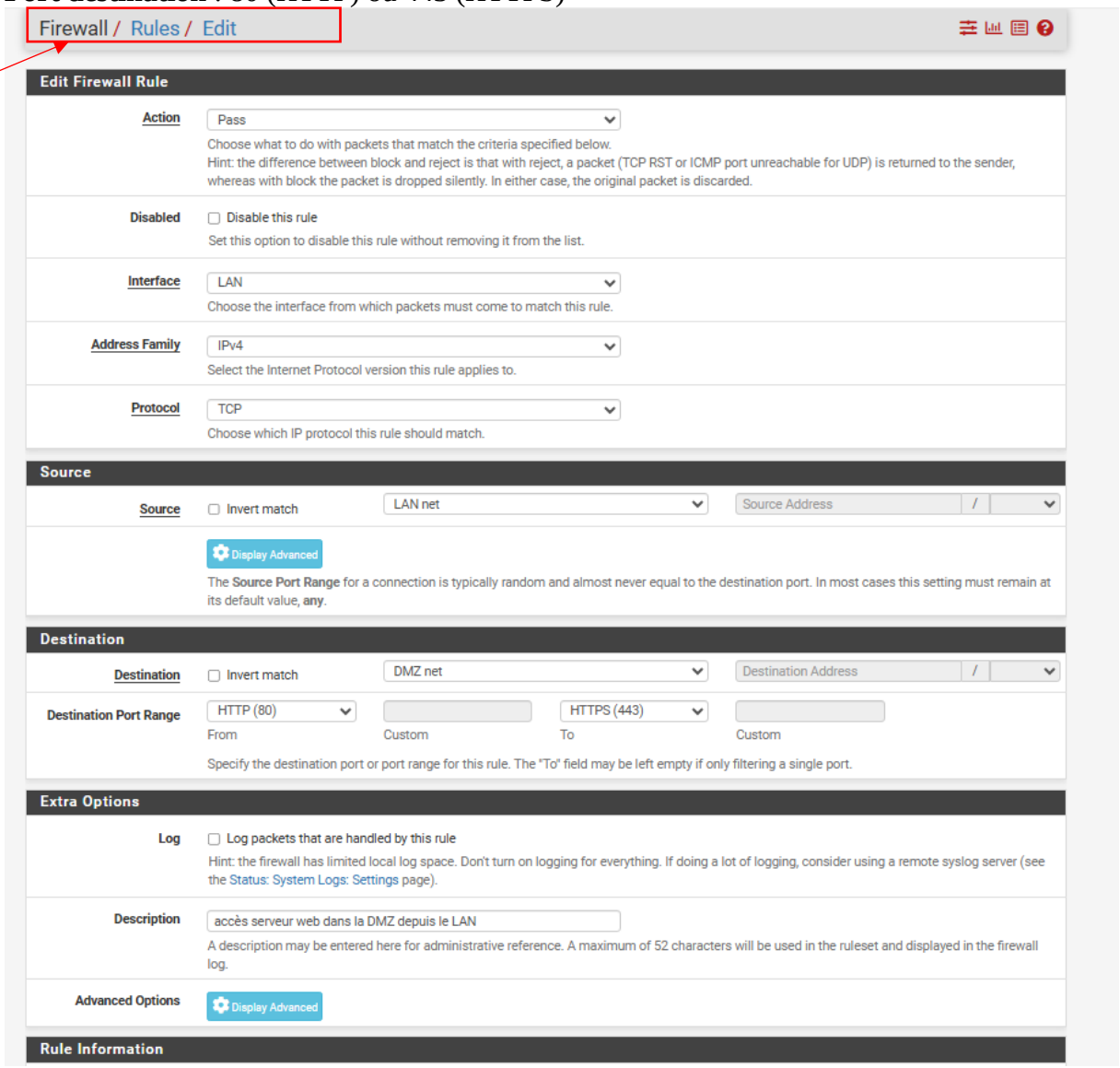
4.3Interface : LAN

4.4Protocol : TCP

4.5Source : LAN net

4.6Destination : IP du serveur web en DMZ

4.7Port destination : 80 (HTTP) ou 443 (HTTPS)

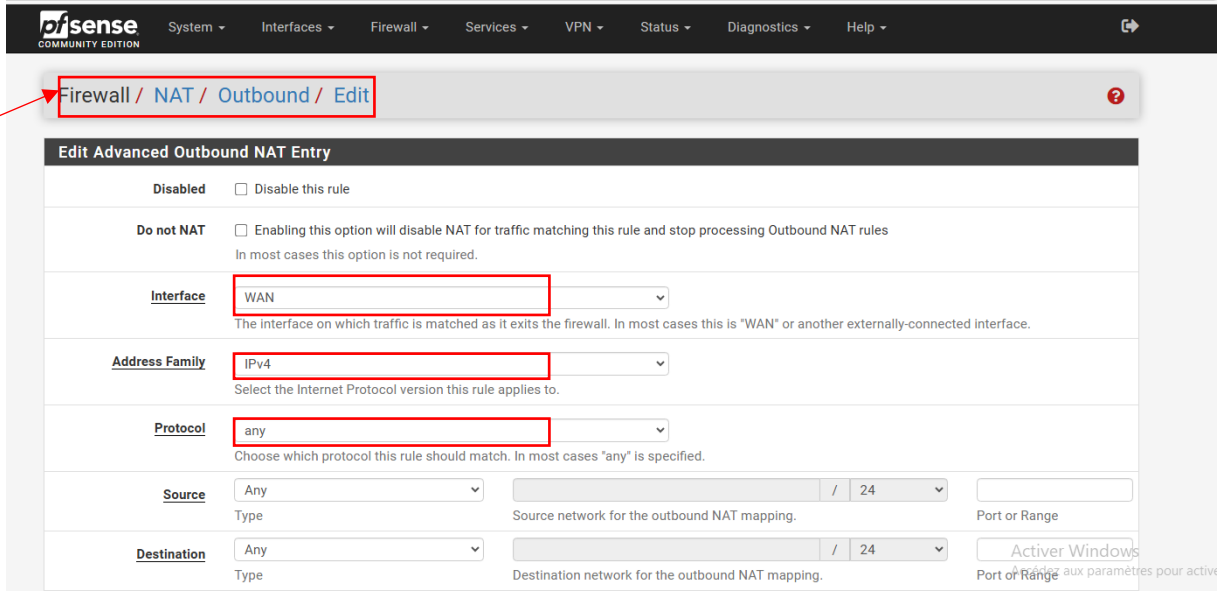


5 Enregistrez et appliquez la règle.

3.4 CONFIGURER LE NAT OUTBOUND POUR AUTORISER LA DMZ A UTILISER LA WAN

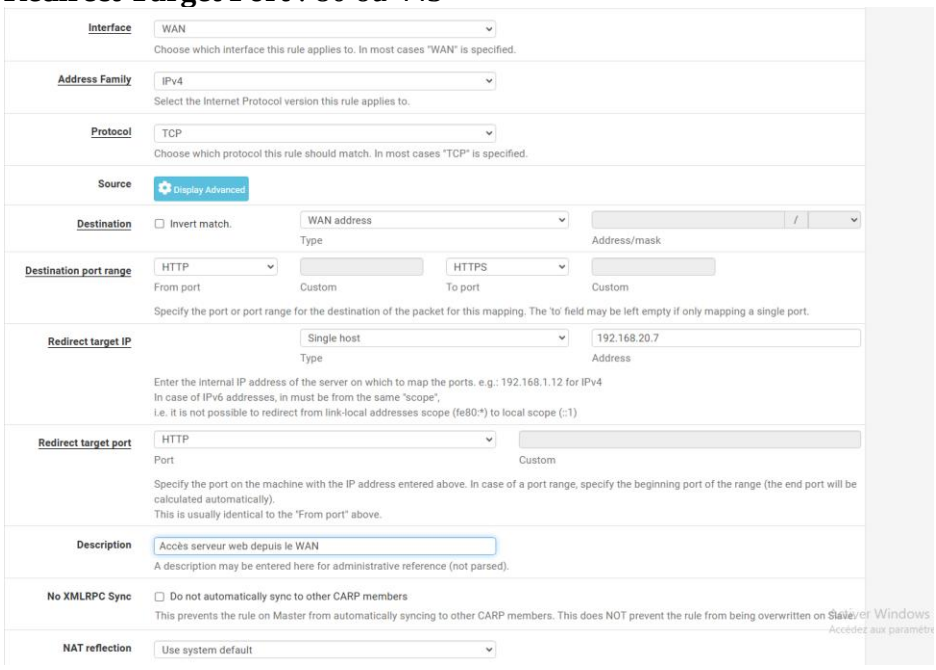
Cette règle permettra au réseau DMZ de « sortir » sur Internet via l'interface WAN.
Pour cela, effectuez les manipulations suivantes :

- Cliquez sur « **Firewall** » - « **NAT** » « **Outbond** » « **Add** » et configurez votre règle ainsi :



3.5 Configurer le NAT pour un accès externe au serveur web en DMZ

1. Allez dans **Firewall > NAT > Port Forward**.
2. Cliquez sur **Add** et configurez la redirection comme suit :
   - **Interface** : WAN
   - **Protocol** : TCP
   - **Destination** : WAN Address
   - **Port destination** : 80 (HTTP) ou 443 (HTTPS)
   - **Redirect Target IP** : IP du serveur web en DMZ
   - **Redirect Target Port** : 80 ou 443



3. Enregistrez et appliquez la règle.

RESUME DES REGLES A CONFIGURER

INTERFACE WAN (rules)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
1/15 KiB	IPv4 TCP	*	*	*	192.168.10.250	80 - 443	*		none	NAT Accès serveur web depuis WAN (NAT)

INTERFACE LAN (rules)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	*	DMZ subnets	80 - 443	*		none	Accès serveur web dans DMZ depuis LAN
0/2.70 MiB	IPv4 *	LAN subnets	*	*	*		*	WANGW	none	Accès internet depuis LAN

INTERFACE DMZ (rules)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
0/456 B	IPv4 *	DMZ subnets	*	*	*	WANGW	none		Accès de la DMZ vers WAN

PORT FORWARDING (NAT)

Port Forward | 1:1 | Outbound | NPt

Rules

Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
WAN	TCP	*	*	WAN address	80 - 443	192.168.10.250	80 - 443	Accès serveur web depuis WAN (NAT)

NAT OUTBOUND

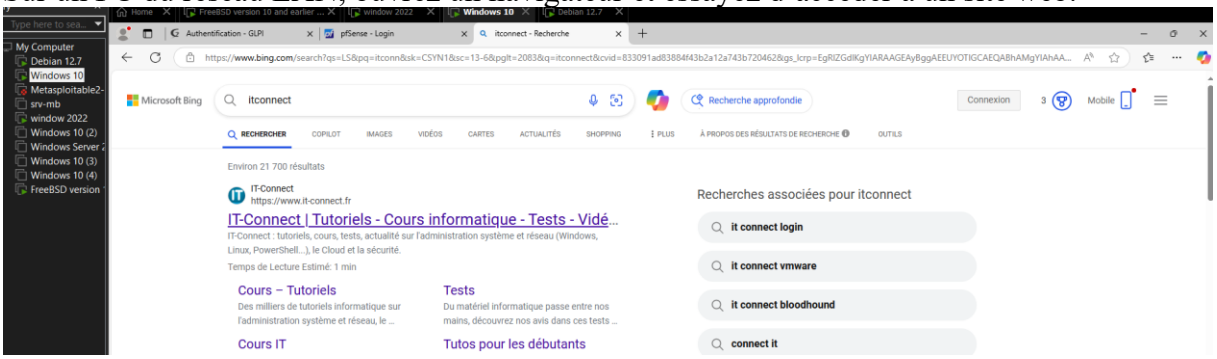
Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
DMZ	DMZ subnets	*	WAN subnets	*	WAN address	*		DMZ accès externe (WAN)

4. Tests et validation

4.1 Tester l'accès à Internet depuis le LAN

- Sur un PC du réseau LAN, ouvrez un navigateur et essayez d'accéder à un site web.

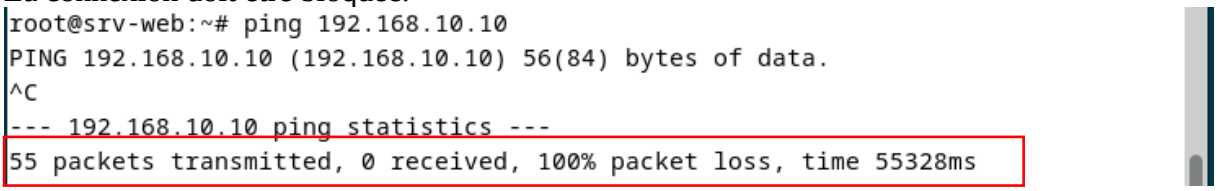


- Si cela ne fonctionne pas, vérifiez les logs de pfSense dans **Status > System Logs > Firewall**.

4.2 Vérifier l'isolation de la DMZ

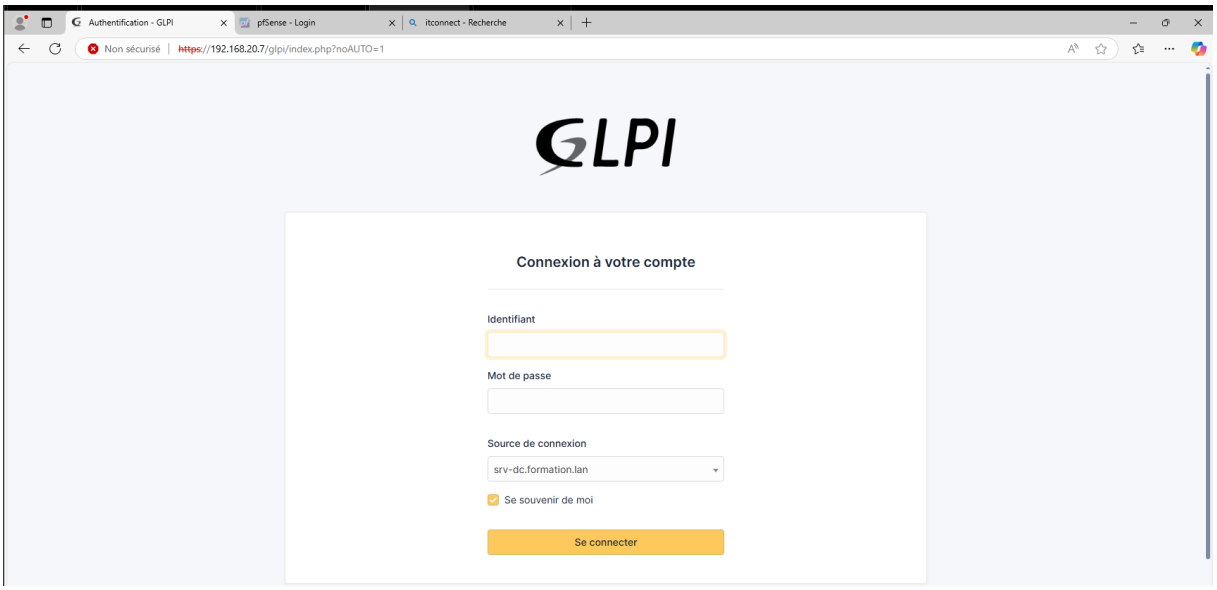
- Depuis une machine en DMZ, essayez de **pinger** une machine en LAN.

- La connexion doit être bloquée.



4.3 Accéder au serveur web depuis le LAN

- Depuis une machine en LAN, ouvrez un navigateur et entrez l'IP du serveur web en DMZ : 192.168.20.7.



4.4 Tester l’accès externe au serveur web en DMZ

- Depuis une connexion externe, tentez d’accéder à l’IP publique de pfSense.

5. Conclusion

Nous avons mis en place un système de filtrage des flux réseau permettant de sécuriser les accès entre les différentes zones de l’infrastructure. Cette configuration garantit un cloisonnement efficace tout en permettant les communications essentielles.