Création de règles de pare-feu pfSense

Sommaire :

I. Présentation de **pfSense** et des ACL :

Dans le cadre de ce projet, j'ai été amené à configurer des **ACL (Access Control Lists)** sur la solution **pfSense**, utilisée comme pare-feu principal au sein de mon infrastructure réseau.

pfSense :

pfSense est une distribution libre et open source basée sur FreeBSD, spécialisée dans la gestion de pare-feu et de routeur. Elle est largement utilisée en entreprise pour sa fiabilité, sa souplesse de configuration, et sa capacité à gérer des réseaux complexes à travers une interface web intuitive.

ACL – Listes de contrôle d'accès :

*Les **ACL (Access Control Lists)** permettent de définir **des règles précises de filtrage** du trafic réseau. Elles servent à **autoriser ou bloquer certains flux** en fonction de plusieurs critères : adresse IP source ou destination, protocole utilisé, port, etc.*

Dans **pfSense**, les ACL sont généralement implémentées via des **rules (règles)** créées sur les interfaces réseau (LAN, DMZ, WAN, etc.). Elles permettent de sécuriser le réseau en maîtrisant finement les communications entre les différents segments (ex. : serveur ↔ client, client ↔ internet, DMZ ↔ LAN...).

II. Objectif du projet :

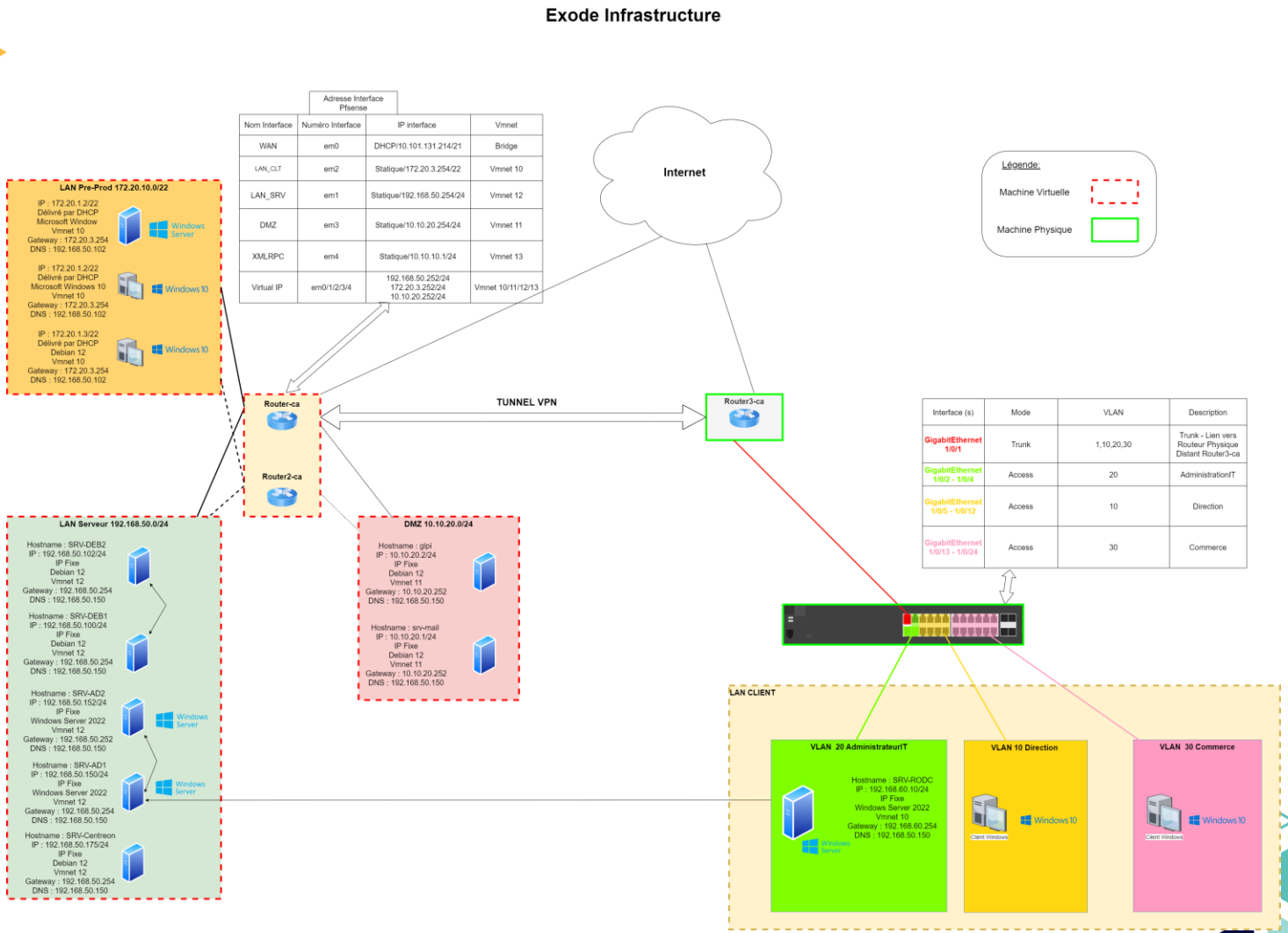
L'objectif de ce projet est de **définir et appliquer des règles de sécurité réseau** via des **ACL (listes de contrôle d'accès)** sur **pfSense**, afin de **protéger l'infrastructure** tout en garantissant le bon fonctionnement des services essentiels.

Plus précisément, ce projet vise à :

- **Contrôler les flux de communication** entre les différentes zones du réseau (LAN, DMZ, WAN),
- **Restreindre l'accès aux services sensibles**, comme les serveurs internes ou l'interface d'administration,
- **Garantir la disponibilité** des services tels que GLPI, le serveur mail ou les sites web hébergés,
- **Limiter les connexions inutiles ou à risque**, notamment en interdisant certains ports, protocoles ou adresses IP,
- **Appliquer le principe du moindre privilège**, en n'autorisant que les communications strictement nécessaires au bon fonctionnement du système.

Un autre aspect essentiel de ce projet est l'utilisation du **filtrage stateful**, propre aux pare-feux comme **pfSense**. Ce type de filtrage permet de **suivre l'état des connexions** (établie, initiée, en réponse...) et d'**autoriser automatiquement le trafic retour** pour une session légitime. Cela évite d'avoir à définir manuellement les règles dans les deux sens et permet une gestion plus fine, plus sécurisée et plus logique des flux réseau.

III. Configuration réseau initiale :



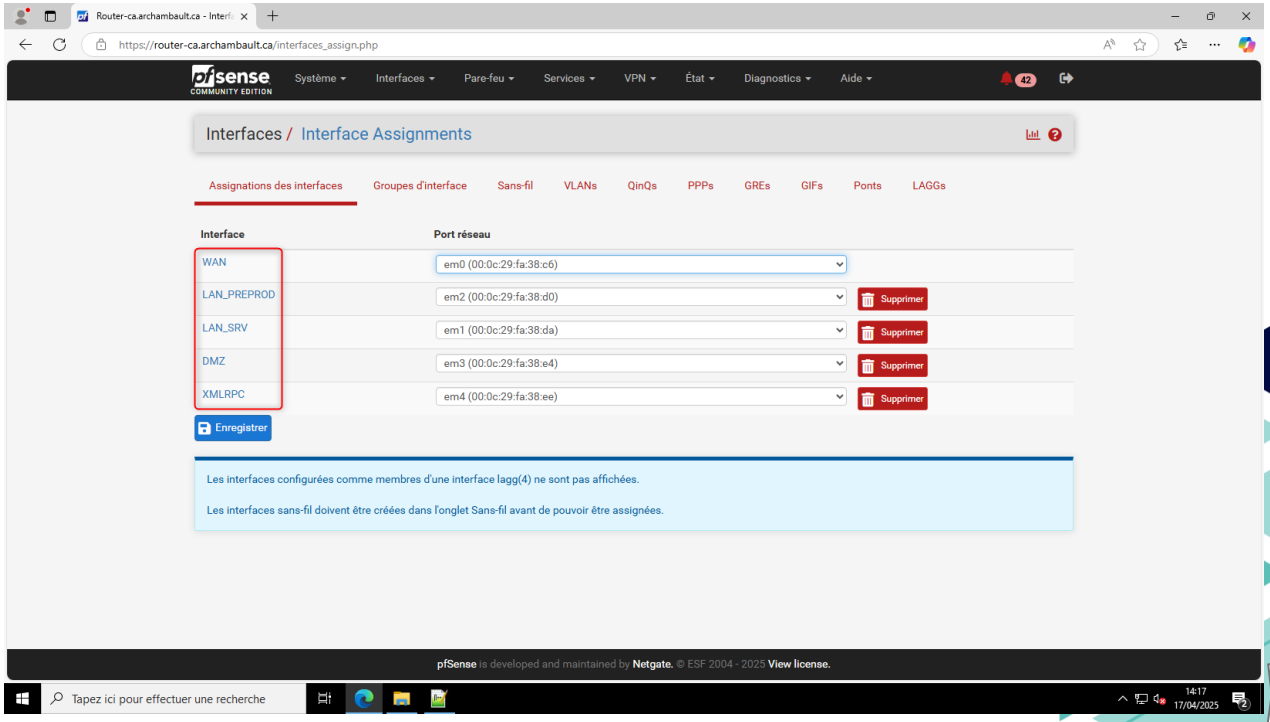
Avant la mise en place des ACL, il est essentiel de présenter la structure réseau en place et le rôle de **pfSense** dans l'architecture.

L'infrastructure repose sur une **topologie segmentée**, organisée autour de trois zones principales :

- **LAN_SRV**: contient les serveurs internes (Active Directory, DNS, DHCP, partages de fichiers, etc.), répartis sur des machines Windows et Linux.
- **LAN PREPROD** : regroupe les serveurs de tests et pc de tests.
- **DMZ (zone démilitarisée)** : héberge les services accessibles depuis l'extérieur comme :
  - Le serveur GLPI (Linux),
  - Le serveur de messagerie (Postfix),

On retrouve également les interfaces :

- **WAN** : interface connectée à Internet, utilisée pour la mise à jour des paquets, l'accès à distance sécurisé, ou encore la réplication **pfSense**.
- **XMLRPC** : interface présente pour la redondance avec le second pare-feu.



IV. Création et mise en place des ACL sur **pfSense** :

Définition des besoins en communication :

Avant de créer les règles, j'ai identifié les flux nécessaires au bon fonctionnement de l'infrastructure, selon le **principe du moindre privilège**.

Voici quelques exemples :

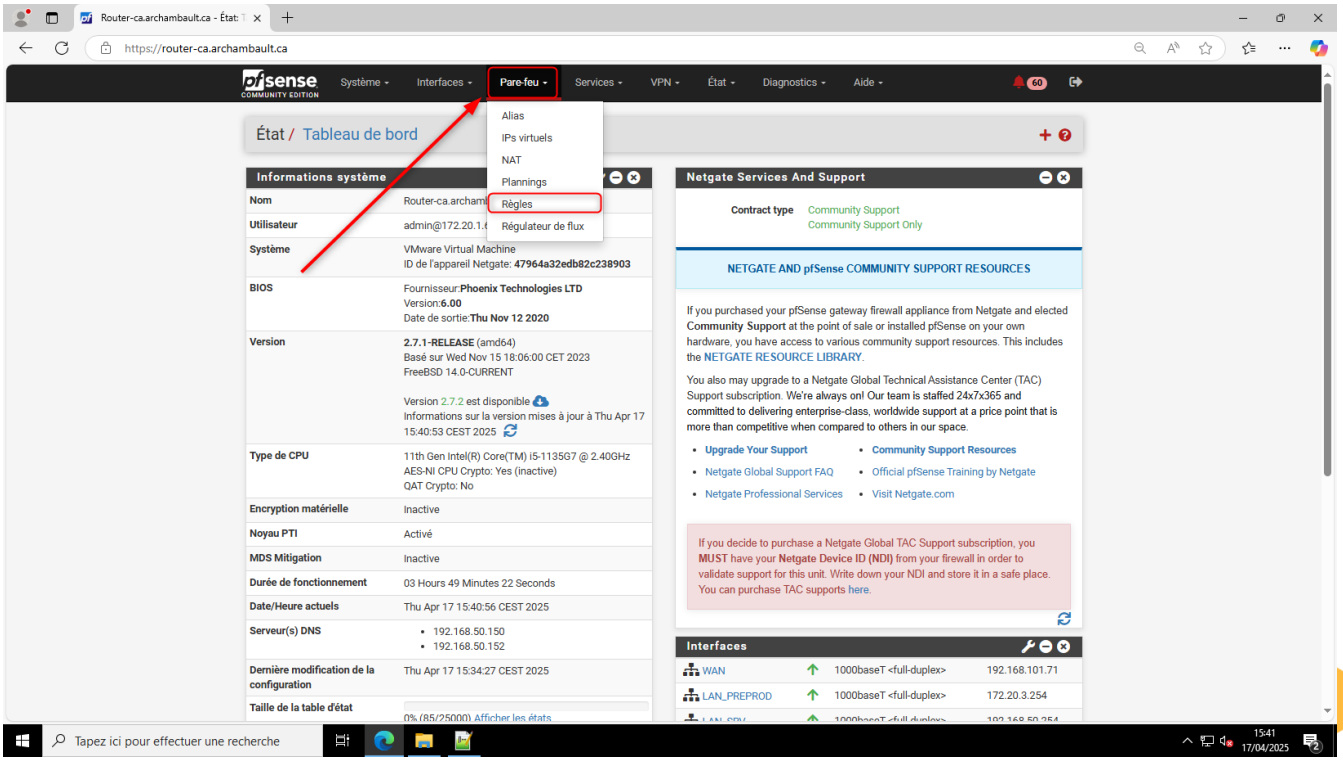
- Les **postes clients (LAN Client)** doivent pouvoir :
  - S'authentifier.
  - Profiter des différences services internes (AD, DNS, fichiers).
  - Consulter GLPI et utiliser le service de mail en DMZ.
  - Accéder à Internet (HTTP/HTTPS).
- Il est également nécessaire d'ajouter une règle de blocage pour éviter toute tentative de connexion sur des ports / protocoles non utilisés dans l'infrastructure.

Création des règles dans **pfSense** :

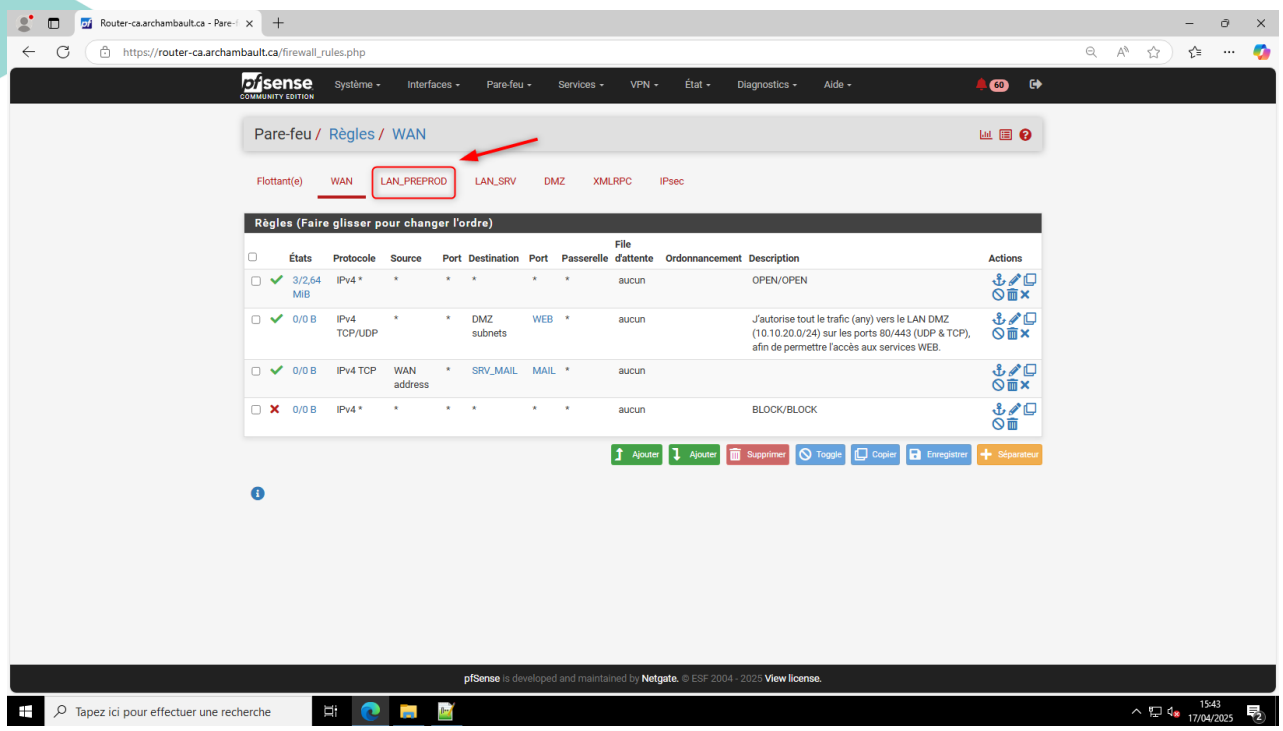
Les ACL ont été créées dans **pfSense** sous forme de rules sur chaque interface, en respectant l'ordre de priorité (du haut vers le bas).

Exemple de création de la règle DNS :

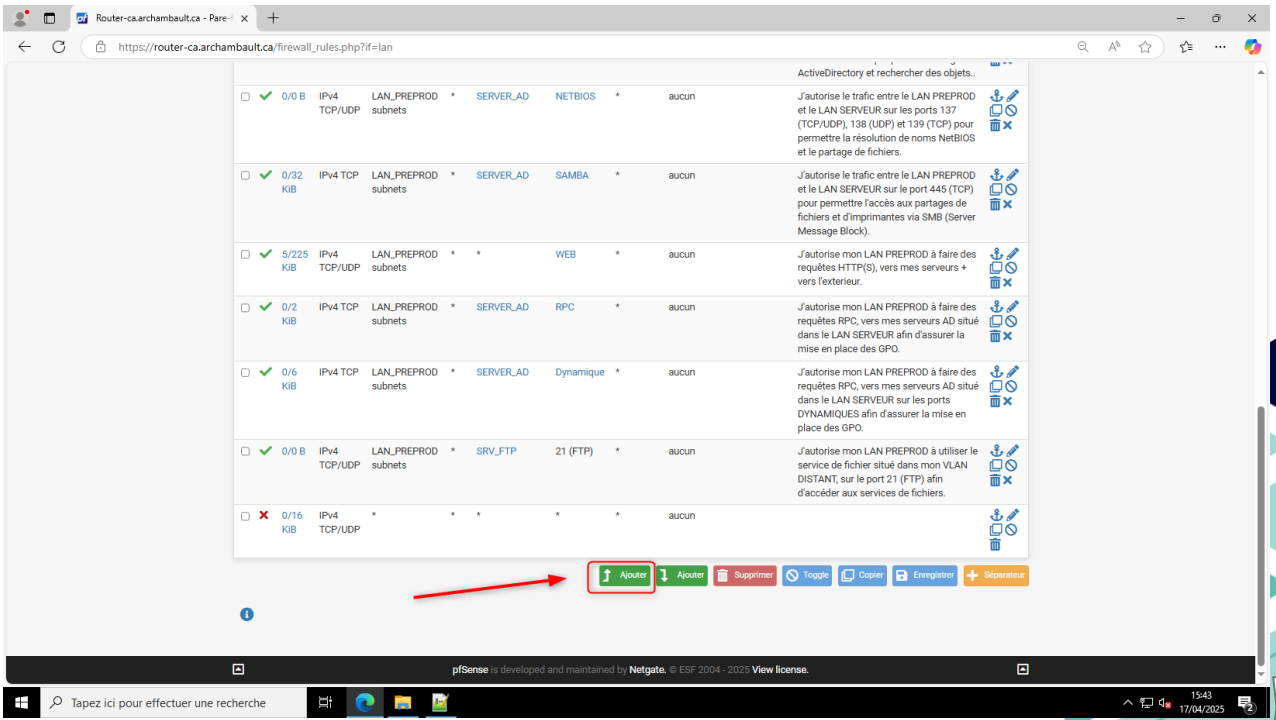
Dans **pfSense** aller dans Pare-feu > Règles et choisir l'interface sur laquelle la règle sera créée. Ici nous choisissons interface LAN_PREPROD afin de créer une règle permettant d'autoriser le LAN_PREPROD a effectuer des requêtes DNS vers mes serveurs DNS situé dans le LAN_SERVEUR.



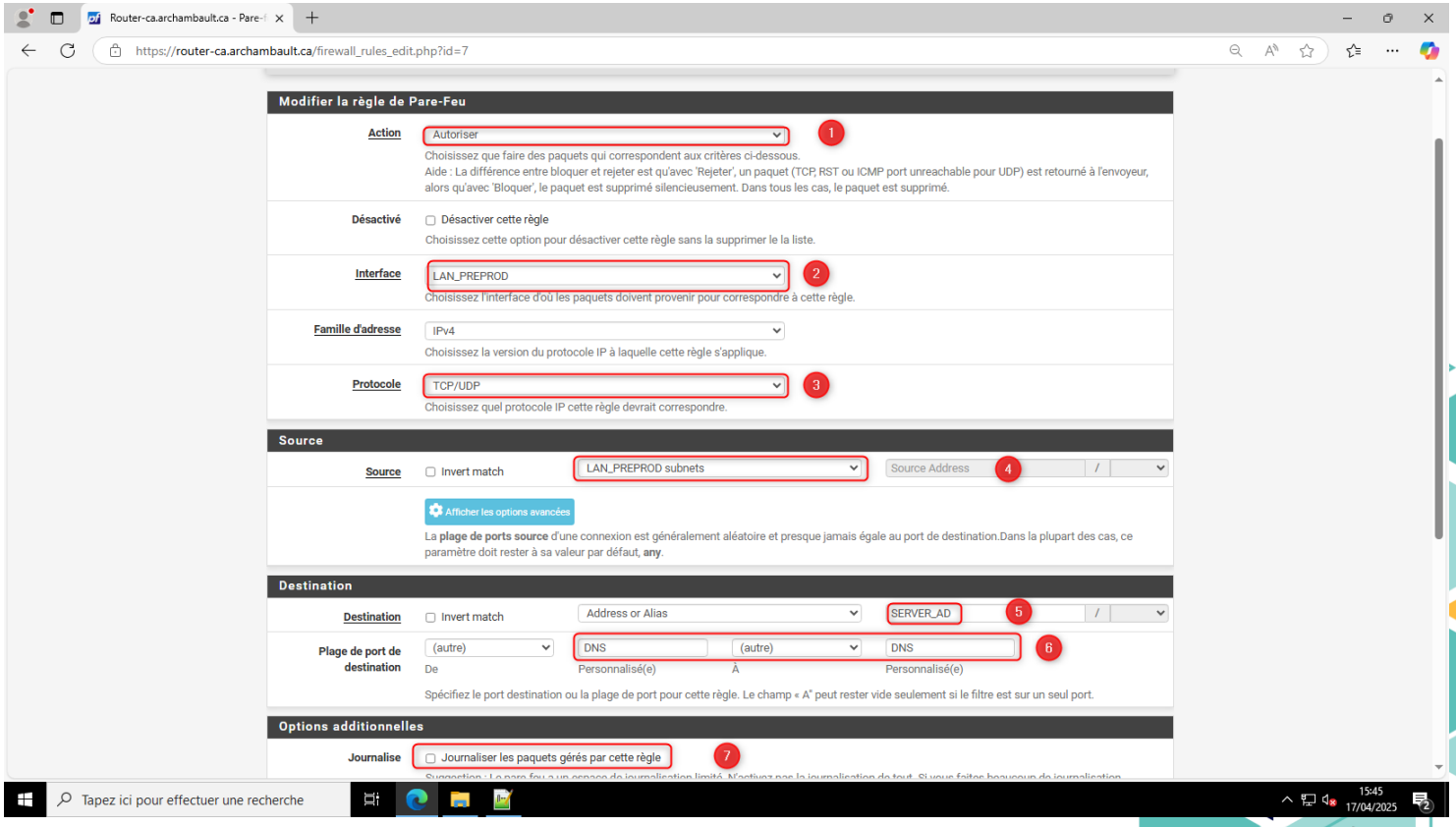
Sélectionner l'interface correspondante, ici LAN_PREPROD.



En bas, cliquer sur Ajouter.

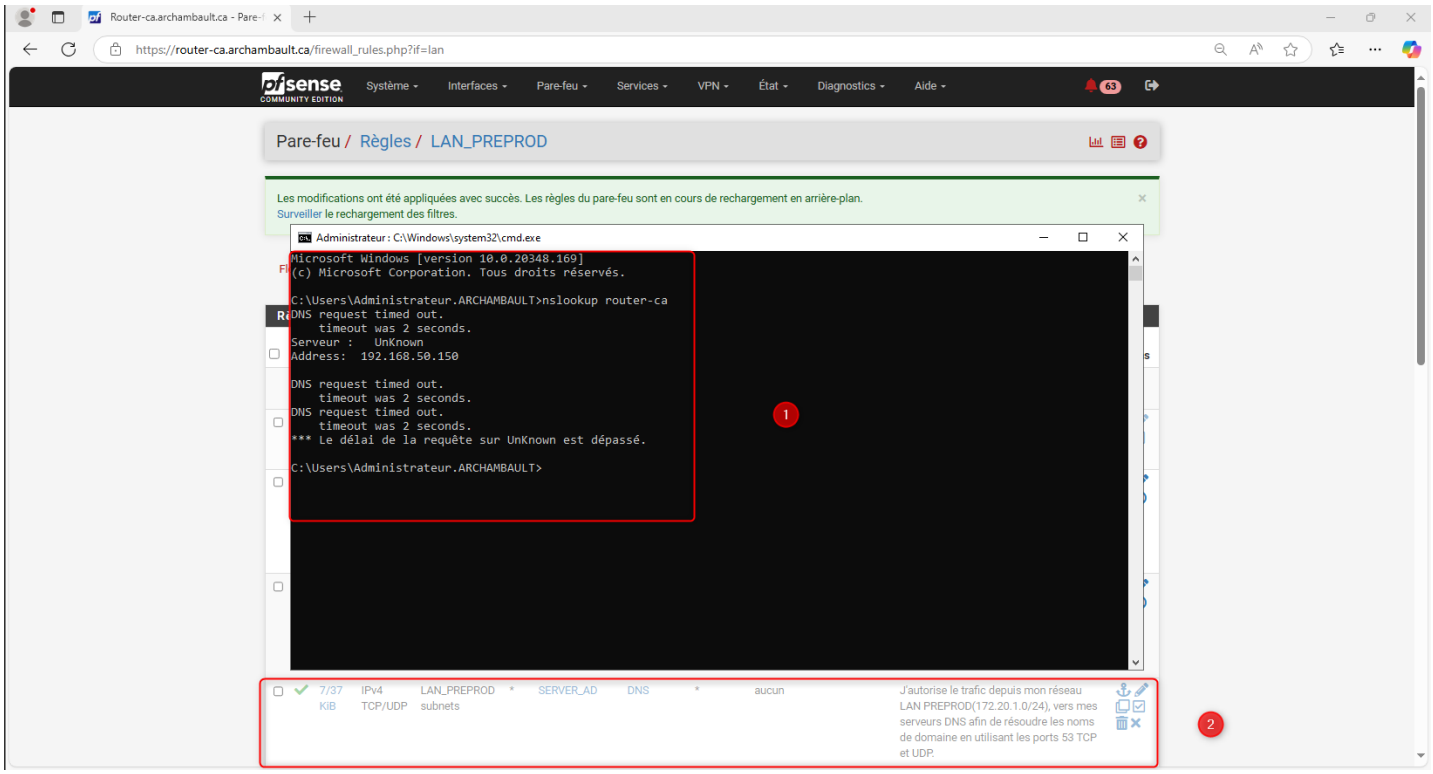


1. Dans un premier temps, cliquer sur Autoriser pour autoriser ce flux.
2. Choisir l'interface ciblée, ici LAN_PREPROD.
3. Choisir le protocole de transport correspondant, ici on mettra TCP/UDP.
4. Saisir la source, ici nous saisirons le réseau entier LAN_PREPROD.
5. Saisir la destination, ici j'ai créé un alias (SERVER_AD), correspondant à mes deux serveurs DNS + AD en redondance).
6. Saisir le port ciblé, ici j'ai créé un alias (DNS), correspondant au port 53.
7. Cocher Journaliser si vous souhaité générer des logs sur cette règle.
8. Enregistrer.

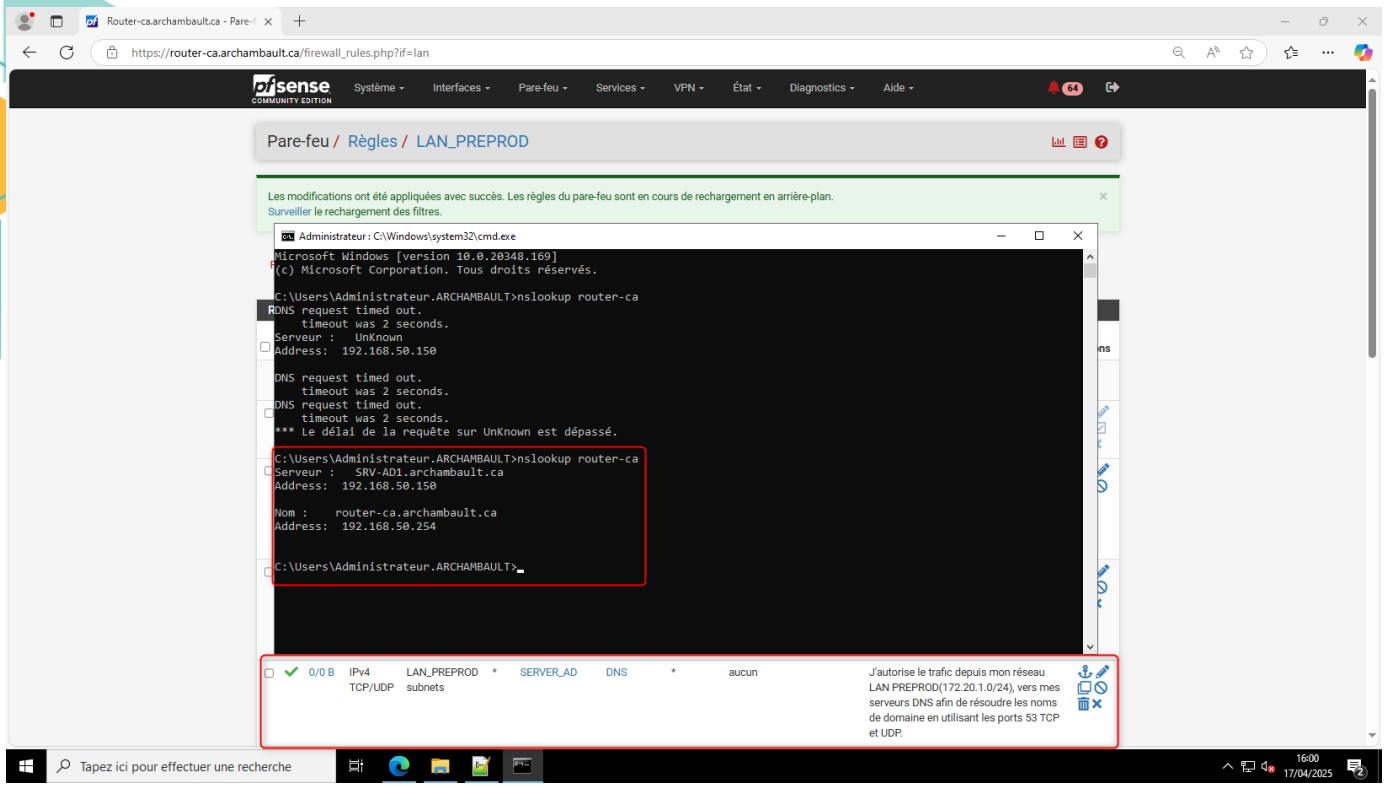


Tests de fonctionnement avec et sans règle :

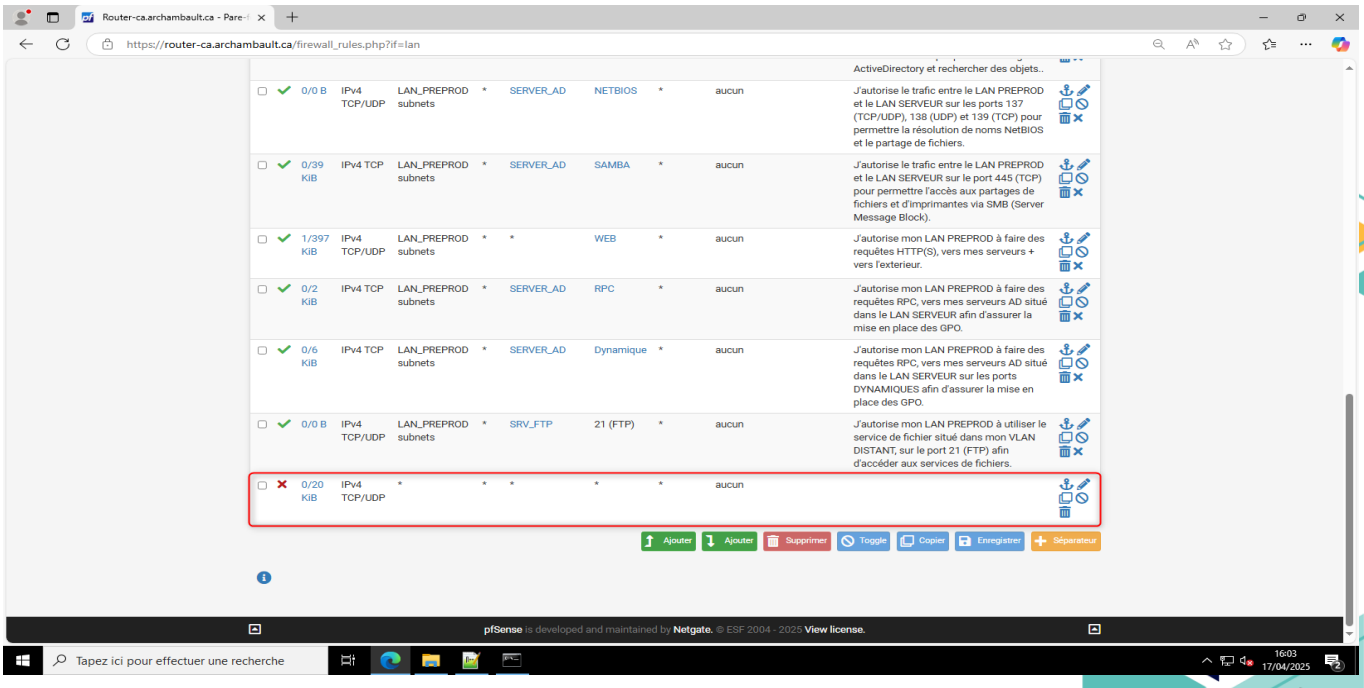
Je bloque la règle dans un premier temps elle apparait grisée donc la résolution DNS ne s'effectue pas.



Dans un second j'active la règle précédemment créée, la résolution est désormais fonctionnelle car ma règle laisse passer uniquement les requêtes DNS depuis mon réseau LAN_PREPROD vers mes serveurs DNS.



De plus, une règle en bas de la liste a été créée afin de bloquer toute autre flux pouvant passer, cette règle va bloquer tout protocole non défini juste au-dessus (priorité des règles).



Explication et application du filtrage stateful :

L'un des grands avantages de **pfSense** est son fonctionnement en **filtrage stateful**, contrairement aux pare-feux statiques.

Le filtrage stateful (filtrage avec suivi d'état) permet à **pfSense** de **suivre le statut de chaque connexion**. Lorsqu'une règle autorise une connexion sortante, **pfSense** crée **automatiquement une règle implicite pour le trafic retour**, uniquement dans le cadre de cette session active.

Exemple avec la règle précédemment créée :

Dans la configuration de l'interface **LAN Préprod**, j'ai eu besoin de permettre aux machines de cette zone d'interroger les **serveurs AD/DNS** internes situés dans le **LAN Serveur**.

Grâce au filtrage stateful de **pfSense** :

- Je n'ai eu besoin de créer qu'une seule règle sur l'interface LAN PREPROD :
  Autoriser les requêtes DNS **vers les IP des serveurs AD/DNS**.
- Aucune règle n'a été nécessaire **dans l'autre sens** (depuis LAN Serveur vers Préprod), car **pfSense** gère automatiquement **le trafic retour** des réponses DNS en suivant l'état de la connexion.

Ce fonctionnement facilite la gestion des règles, **réduit les risques d'erreurs** (pas de double saisie), et **améliore la sécurité**, car seuls les retours de connexions initiées sont autorisés.

V. Compétences mises en œuvre :

Compétence du référentiel	**Mise en œuvre dans le projet**
Gérer le patrimoine informatique	Analyse des flux réseau nécessaires entre les différentes zones (LAN, DMZ, WAN, PREPROD). Organisation logique des règles ACL dans **pfSense**.
Organiser son développement professionnel	Approfondissement des connaissances sur les pare-feux stateful, la gestion des interfaces réseau dans **pfSense** et la logique de filtrage orientée service.
Mettre à disposition des utilisateurs un service informatique	Création de règles de filtrage permettant l'accès aux services essentiels (DNS, web, messagerie, etc.) tout en garantissant la sécurité de l'infrastructure.

VI. Diagramme :