



Création de règles de pare-feu  
pfSense



## Sommaire :

- I. Présentation de **pfSense** et des ACL
- II. Objectif du projet
- III. Création et mise en place des ACL sur **pfSense**
- IV. Compétences mises en œuvre
- V. Diagramme

## 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.

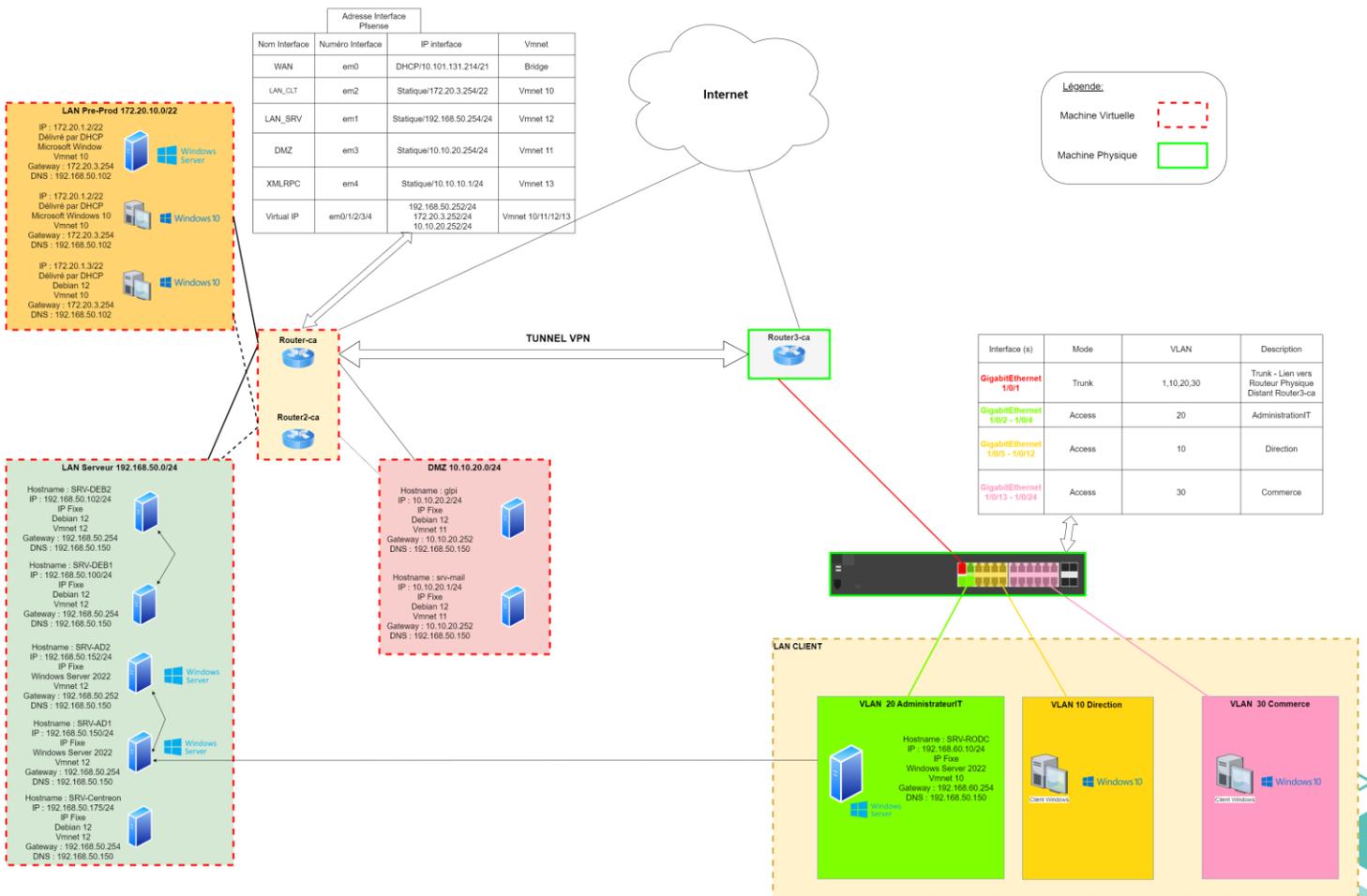
Plus précisément, ce projet vise à :

- **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 :

#### Exode Infrastructure



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.

Interface	Port réseau
WAN	em0 (00:0c:29:fa:38:c6)
LAN_PREPROD	em2 (00:0c:29:fa:38:d0) <span>Supprimer</span>
LAN_SRV	em1 (00:0c:29:fa:38:da) <span>Supprimer</span>
DMZ	em3 (00:0c:29:fa:38:e4) <span>Supprimer</span>
XMLRPC	em4 (00:0c:29:fa:38:ee) <span>Supprimer</span>

Enregistrer

Les interfaces configurées comme membres d'une interface lagg(4) ne sont pas affichées.  
Les interfaces sans-fil doivent être créées dans l'onglet Sans-fil avant de pouvoir être assignées.

#### 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 :

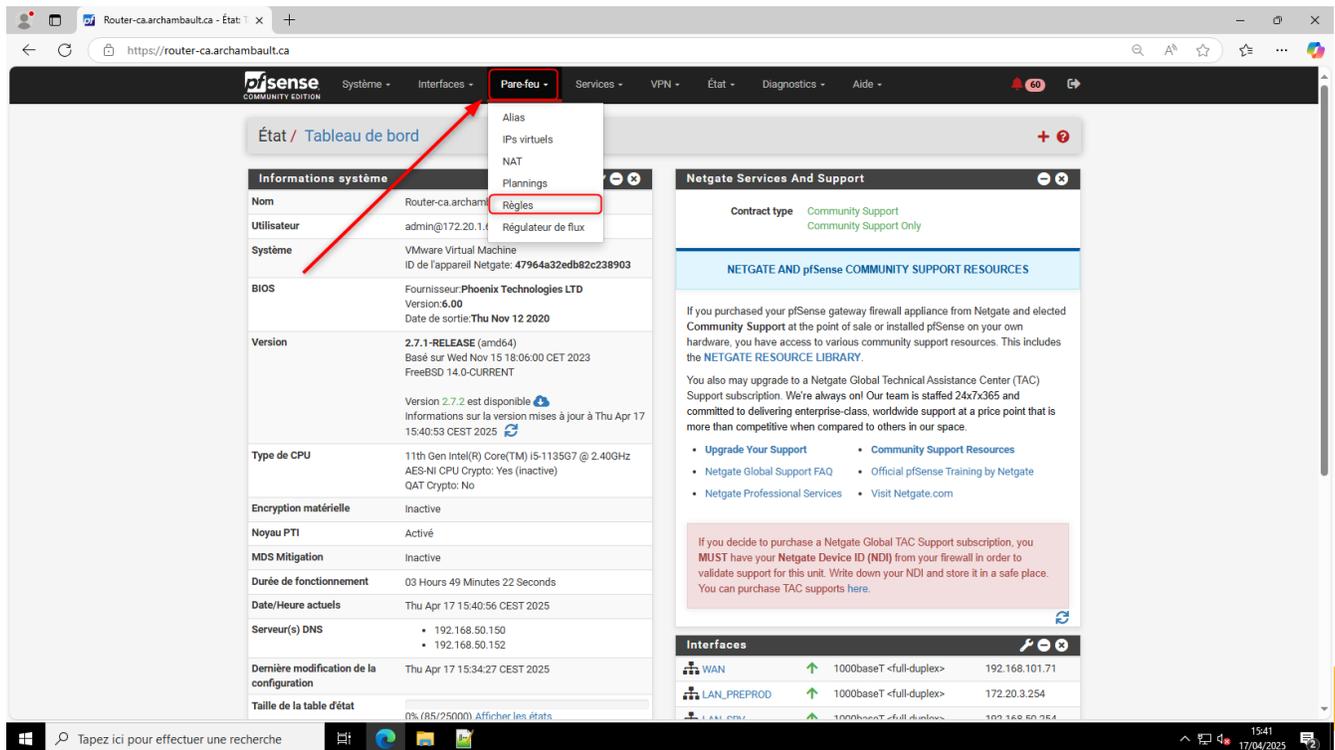
- Les **postes clients (LAN Client)** doivent pouvoir :
  - S'authentifier.
  - Profiter des différences services internes (AD, DNS, fichiers).
  - Consulter GLPI et utiliser le service de mail en DMZ.
  - Accéder à Internet (HTTP/HTTPS).
- Il est également nécessaire d'ajouter une règle de blocage pour 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 règles 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 à effectuer des requêtes DNS vers mes serveurs DNS situé dans le LAN\_SERVEUR.



The screenshot shows the pfSense web interface. The 'Pare-feu' (Firewall) menu is open, and the 'Règles' (Rules) option is highlighted with a red box. A red arrow points from the 'Règles' option to the 'Informations système' (System Information) section. The 'Informations système' section displays various system details, including the user 'admin@172.20.3.254', the system name 'Router-ca-archambault.ca', and the version '2.7.1-RELEASE (amd64)'. The 'Serveur(s) DNS' (DNS Server(s)) section lists two IP addresses: 192.168.50.150 and 192.168.50.152. The 'Interfaces' section at the bottom shows the 'LAN\_PREPROD' interface with IP address 172.20.3.254.

Informations système	
Nom	Router-ca-archambault.ca
Utilisateur	admin@172.20.3.254
Système	VMware Virtual Machine ID de l'appareil Netgate: 47964a32edb82c238903
BIOS	Fournisseur: Phoenix Technologies LTD Version: 6.00 Date de sortie: Thu Nov 12 2020
Version	2.7.1-RELEASE (amd64) Basé sur Wed Nov 15 18:06:00 CET 2023 FreeBSD 14.0-CURRENT  Version 2.7.2 est disponible Informations sur la version mises à jour à Thu Apr 17 15:40:53 CEST 2025
Type de CPU	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Encryption matérielle	Inactive
Noyau PTI	Activé
MDS Mitigation	Inactive
Durée de fonctionnement	03 Hours 49 Minutes 22 Seconds
Date/Heure actuels	Thu Apr 17 15:40:56 CEST 2025
Serveur(s) DNS	<ul style="list-style-type: none"><li>192.168.50.150</li><li>192.168.50.152</li></ul>
Dernière modification de la configuration	Thu Apr 17 15:34:27 CEST 2025
Taille de la table d'état	0% (85/25000) Afficher les états

Interfaces		
WAN	↑ 1000baseT <full-duplex>	192.168.101.71
LAN_PREPROD	↑ 1000baseT <full-duplex>	172.20.3.254
LAN_SERVEUR	↑ 1000baseT <full-duplex>	192.168.50.254

Sélectionner l'interface correspondante, ici LAN\_PREPROD.

The screenshot shows the pfSense web interface for configuring firewall rules. The breadcrumb navigation is "Pare-feu / Règles / WAN". Below this, there are tabs for different interfaces: "Flottant(e)", "WAN", "LAN\_PREPROD" (which is selected and highlighted with a red box), "LAN\_SRV", "DMZ", "XMLRPC", and "IPsec". A table of rules is displayed with columns: "États", "Protocole", "Source", "Port", "Destination", "Port", "Passerelle", "File d'attente", "Ordonnement", "Description", and "Actions". The first rule is "OPEN/OPEN" with protocol "IPv4\*" and source "3/2,64 MIB". The second rule is "J'autorise tout le trafic (any) vers le LAN DMZ" with protocol "IPv4 TCP/UDP", source "subnets", and destination "DMZ subnets". The third rule is "J'autorise mon LAN PREPROD à faire des requêtes HTTP(S)" with protocol "IPv4 TCP", source "WAN address", and destination "SRV\_MAIL MAIL". The fourth rule is "BLOCK/BLOCK" with protocol "IPv4\*". At the bottom of the table, there are buttons: "Ajouter", "Ajouter", "Supprimer", "Toggle", "Copier", "Enregistrer", and "Séparateur". A red arrow points to the "LAN\_PREPROD" tab.

En bas, cliquer sur Ajouter.

This screenshot shows the same pfSense interface but with a list of rules. The "Ajouter" button at the bottom is highlighted with a red box and a red arrow. The rules listed are:

- ActiveDirectory et rechercher des objets.
- J'autorise le trafic entre le LAN PREPROD et le LAN SERVEUR sur les ports 137 (TCP/UDP), 138 (UDP) et 139 (TCP) pour permettre la résolution de noms NetBIOS et le partage de fichiers.
- J'autorise le trafic entre le LAN PREPROD et le LAN SERVEUR sur le port 445 (TCP) pour permettre l'accès aux partages de fichiers et d'imprimantes via SMB (Server Message Block).
- J'autorise mon LAN PREPROD à faire des requêtes HTTP(S), vers mes serveurs + vers l'extérieur.
- J'autorise mon LAN PREPROD à faire des requêtes RPC, vers mes serveurs AD situés dans le LAN SERVEUR afin d'assurer la mise en place des GPO.
- J'autorise mon LAN PREPROD à faire des requêtes RPC, vers mes serveurs AD situés dans le LAN SERVEUR sur les ports DYNAMIQUES afin d'assurer la mise en place des GPO.
- J'autorise mon LAN PREPROD à utiliser le service de fichier situé dans mon VLAN DISTANT, sur le port 21 (FTP) afin d'accéder aux services de fichiers.

The "Ajouter" button is highlighted with a red box and a red arrow.

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 saisissons 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 souhaitez générer des logs sur cette règle.
8. Enregistrer.

**Modifier la règle de Pare-Feu**

**Action**  1  
Choisissez que faire des paquets qui correspondent aux critères ci-dessous.  
Aide : La différence entre bloquer et rejeter est qu'avec 'Rejeter', un paquet (TCP, RST ou ICMP port unreachable pour UDP) est retourné à l'envoyeur, alors qu'avec 'Bloquer', le paquet est supprimé silencieusement. Dans tous les cas, le paquet est supprimé.

**Désactivé**  Désactiver cette règle  
Choisissez cette option pour désactiver cette règle sans la supprimer de la liste.

**Interface**  2  
Choisissez l'interface d'où les paquets doivent provenir pour correspondre à cette règle.

**Famille d'adresse**   
Choisissez la version du protocole IP à laquelle cette règle s'applique.

**Protocole**  3  
Choisissez quel protocole IP cette règle devrait correspondre.

**Source**

**Source**  Invert match  4 / Source Address

[Afficher les options avancées](#)

La plage de ports source d'une connexion est généralement aléatoire et presque jamais égale au port de destination. Dans la plupart des cas, ce paramètre doit rester à sa valeur par défaut, any.

**Destination**

**Destination**  Invert match  5 / Address or Alias

**Plage de port de destination**

De  (autre) À  (autre) 6  
Personnalisé(e) Personnalisé(e)

Spécifiez le port destination ou la plage de port pour cette règle. Le champ « A » peut rester vide seulement si le filtre est sur un seul port.

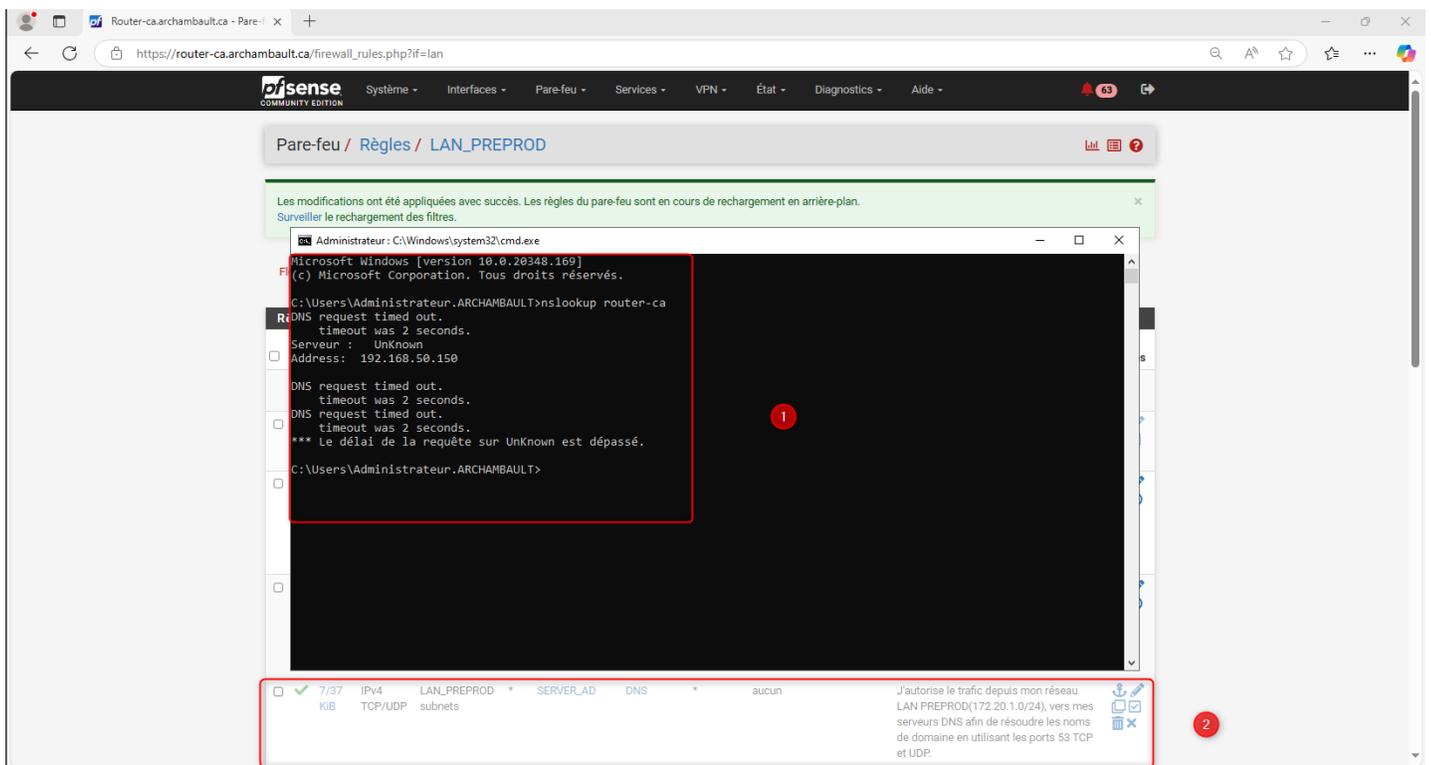
**Options additionnelles**

**Journalise**  Journaliser les paquets gérés par cette règle 7

Journalisation : La pare-feu a un espace de journalisation limité. Modifiez pas la journalisation de tout. SI vous faites beaucoup de journalisation

## 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.



The screenshot shows the pfSense firewall configuration interface. The page title is "Pare-feu / Règles / LAN\_PREPROD". A green notification bar at the top states: "Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan. Surveiller le rechargement des filtres." Below this, a terminal window is open, showing the command prompt "C:\Users\Administrateur.ARCHAMBAULT>nslookup router-ca". The output of the command is as follows:

```
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.ARCHAMBAULT>nslookup router-ca
R:
DNS request timed out.
    timeout was 2 seconds.
Server:      Unknown
Address: 192.168.50.150

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Le délai de la requête sur Unknown est dépassé.
C:\Users\Administrateur.ARCHAMBAULT>
```

Below the terminal window, a table of firewall rules is visible. The rule "LAN\_PREPROD" is highlighted with a red box. The table has the following columns: "7/37", "IPv4", "LAN\_PREPROD", "SERVER\_AD", "DNS", "aucun", and "J'autorise le trafic depuis mon réseau LAN PREPROD(172.20.1.0/24), vers mes serveurs DNS afin de résoudre les noms de domaine en utilisant les ports 53 TCP et UDP." The rule is currently disabled, as indicated by the greyed-out state.

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.

Router-ca.archambault.ca - Pare-feu

https://router-ca.archambault.ca/firewall\_rules.php?f=lan

Pare-feu / Règles / LAN\_PREPROD

Les modifications ont été appliquées avec succès. Les règles du pare-feu sont en cours de rechargement en arrière-plan. Surveiller le rechargement des filtres.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur.ARCHAMBAULT>nslookup router-ca
DNS request timed out.
timeout was 2 seconds.
Server: Unknown
Address: 192.168.50.150

DNS request timed out.
timeout was 2 seconds.
DNS request timed out.
timeout was 2 seconds.
*** Le délai de la requête sur Unknown est dépassé.

C:\Users\Administrateur.ARCHAMBAULT>nslookup router-ca
Server: SRV-AD1.archambault.ca
Address: 192.168.50.150

Nom : router-ca.archambault.ca
Address: 192.168.50.254

C:\Users\Administrateur.ARCHAMBAULT>

```

<input checked="" type="checkbox"/>	0/0 B	IPv4	LAN_PREPROD	*	SERVER_AD	DNS	*	aucun	J'autorise le trafic depuis mon réseau LAN PREPROD(172.20.1.0/24), vers mes serveurs DNS afin de résoudre les noms de domaine en utilisant les ports 53 TCP et UDP.
-------------------------------------	-------	------	-------------	---	-----------	-----	---	-------	---

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).

Router-ca.archambault.ca - Pare-feu

https://router-ca.archambault.ca/firewall\_rules.php?f=lan

<input checked="" type="checkbox"/>	0/0 B	IPv4	LAN_PREPROD	*	SERVER_AD	NETBIOS	*	aucun	ActiveDirectory et recherche des objets. J'autorise le trafic entre le LAN PREPROD et le LAN SERVEUR sur les ports 137 (TCP/UDP), 138 (UDP) et 139 (TCP) pour permettre la résolution de noms NetBIOS et le partage de fichiers.
<input checked="" type="checkbox"/>	0/39 KIB	IPv4	LAN_PREPROD	*	SERVER_AD	SAMBA	*	aucun	J'autorise le trafic entre le LAN PREPROD et le LAN SERVEUR sur le port 445 (TCP) pour permettre l'accès aux partages de fichiers et d'imprimantes via SMB (Server Message Block).
<input checked="" type="checkbox"/>	1/397 KIB	IPv4	LAN_PREPROD	*	*	WEB	*	aucun	J'autorise mon LAN PREPROD à faire des requêtes HTTP(S), vers mes serveurs + vers l'extérieur.
<input checked="" type="checkbox"/>	0/2 KIB	IPv4	LAN_PREPROD	*	SERVER_AD	RPC	*	aucun	J'autorise mon LAN PREPROD à faire des requêtes RPC, vers mes serveurs AD situés dans le LAN SERVEUR afin d'assurer la mise en place des GPO.
<input checked="" type="checkbox"/>	0/6 KIB	IPv4	LAN_PREPROD	*	SERVER_AD	Dynamique	*	aucun	J'autorise mon LAN PREPROD à faire des requêtes RPC, vers mes serveurs AD situés dans le LAN SERVEUR sur les ports DYNAMIQUES afin d'assurer la mise en place des GPO.
<input checked="" type="checkbox"/>	0/0 B	IPv4	LAN_PREPROD	*	SRV_FTP	21 (FTP)	*	aucun	J'autorise mon LAN PREPROD à utiliser le service de fichier situé dans mon VLAN DISTANT, sur le port 21 (FTP) afin d'accéder aux services de fichiers.
<input checked="" type="checkbox"/>	0/20 KIB	IPv4	LAN_PREPROD	*	*	*	*	aucun	

Ajouter Ajouter Supprimer Toggle Copier Enregistrer Séparer

pfSense is developed and maintained by Netgate. © ESP 2004 - 2025 View license.

## 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 :

<b>Compétence du référentiel</b>	<b>Mise en œuvre dans le projet</b>
Gérer le patrimoine informatique	Analyse des flux réseau nécessaires entre les différentes zones (LAN, DMZ, WAN, PREPROD). Organisation logique des règles ACL dans <b>pfSense</b> .
Organiser son développement professionnel	Approfondissement des connaissances sur les pare-feux stateful, la gestion des interfaces réseau dans <b>pfSense</b> 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 :

### CRÉATION DES RÈGLES DE PARE-FEU PFSENSE

