DOMOTech

CONFIGURATION DE PFSENSE

PROCEDURE

Date de création : 01/03/2022
Version : 1.1
Pour validation : DSI
A destination : DSI
Mode de diffusion : SharePoint
Nombre de pages : 15

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau	1.0	Initialisation du document
Dylan Chau	1.1	Mise à jour

Validation			
Rédacteur		Validateur	
Nom	Date	Nom	Date
Dylan Chau	01/03/2023	DSI	01/03/2023
Date d'application : 01/03/2023			

Sommaire

Prérequis

- Un routeur/FW PFSense avec une carte réseau WAN, et les cartes réseaux LAN (au moins une). Dans notre cas, il s'agit du réseau DMT SRV et DMT USER.
- La matrice de flux des services DOMOTech.

Présentation

pfSense est une solution de pare-feu et de routage open-source basée sur le système d'exploitation FreeBSD. Il offre une multitude de fonctionnalités avancées pour sécuriser et gérer les réseaux informatiques de toutes tailles, allant des petites entreprises aux environnements d'entreprise complexes.

Parmi ses fonctionnalités, on peut retrouver :

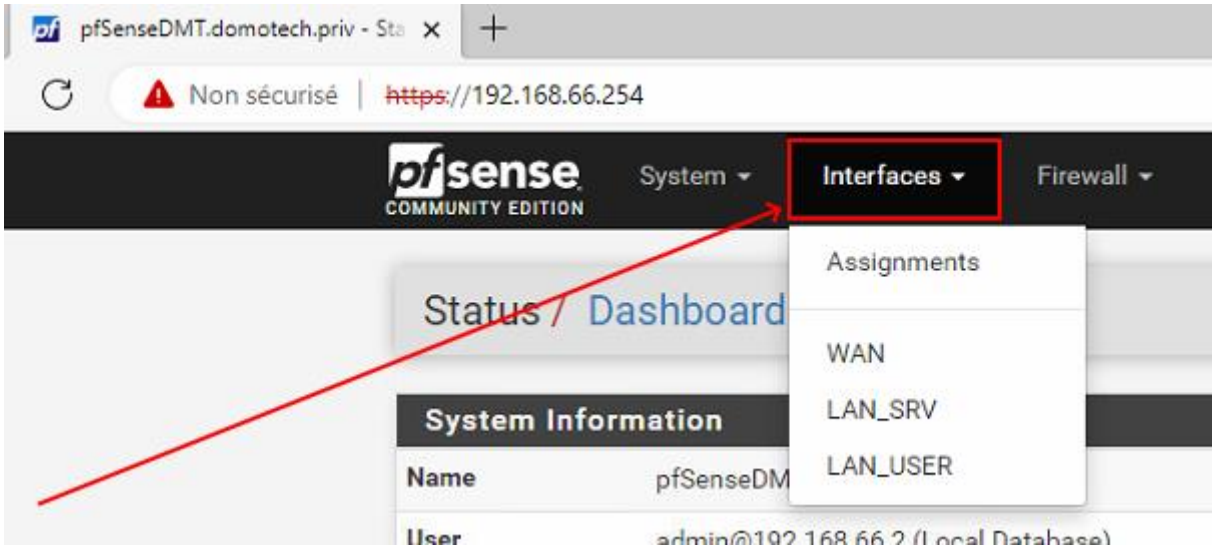
- Pare-feu
- Routage
- VPN
- Journalisation et surveillance

I) Création des interfaces réseaux

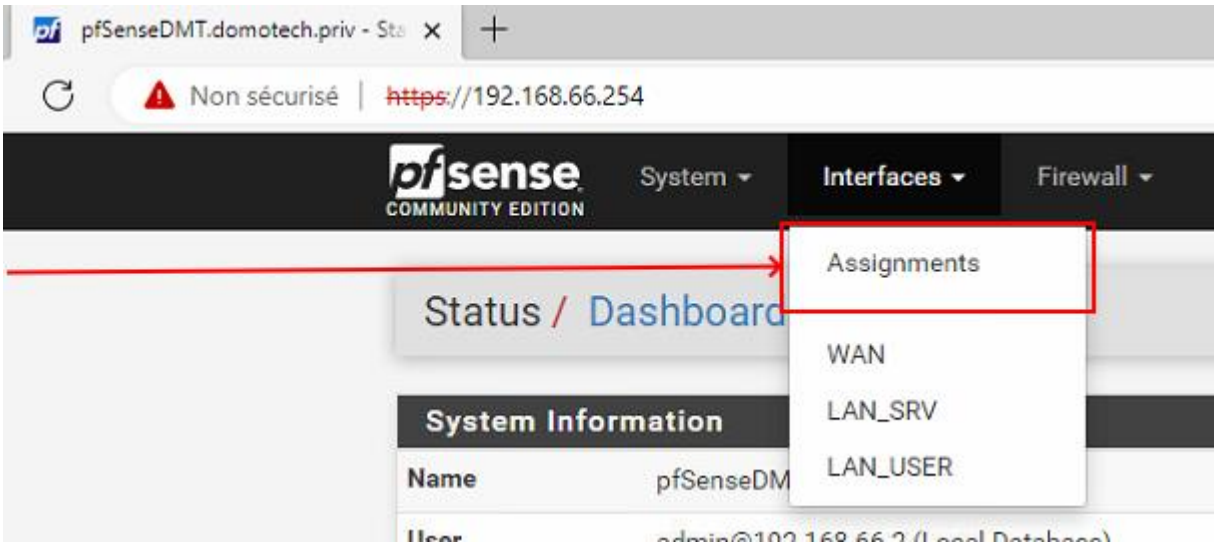
Nous allons créer l'ensemble des interfaces réseaux afin de permettre la connectivité entre les différents LANs.

/!\ Il est important d'avoir une carte réseau LAN configuré afin de pouvoir accéder à l'interface PFSense et de configurer les autres.

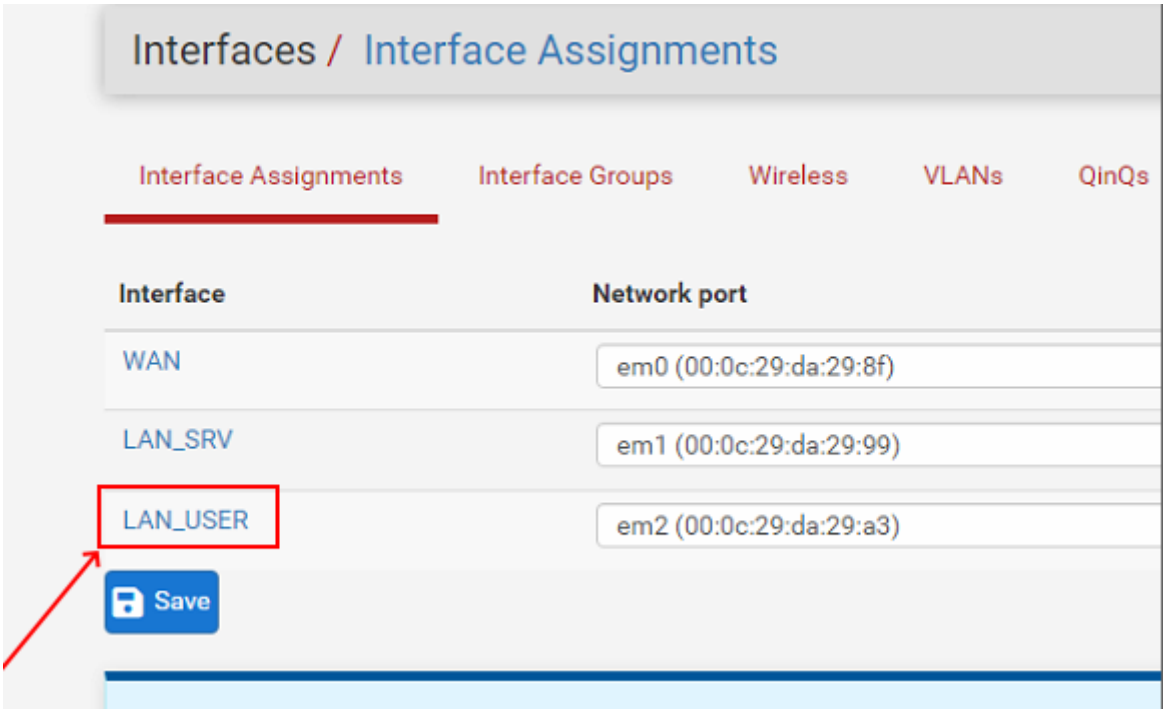
- Cliquer sur « Interfaces ».



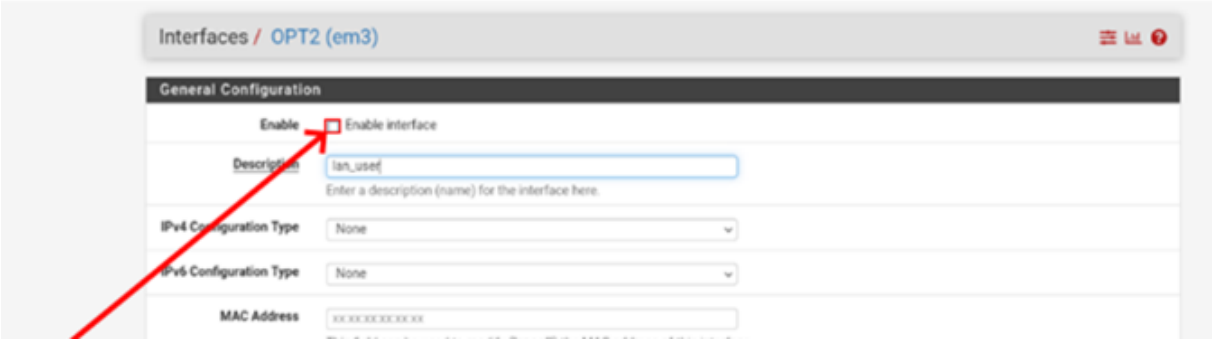
- Cliquer sur « Assignements ».



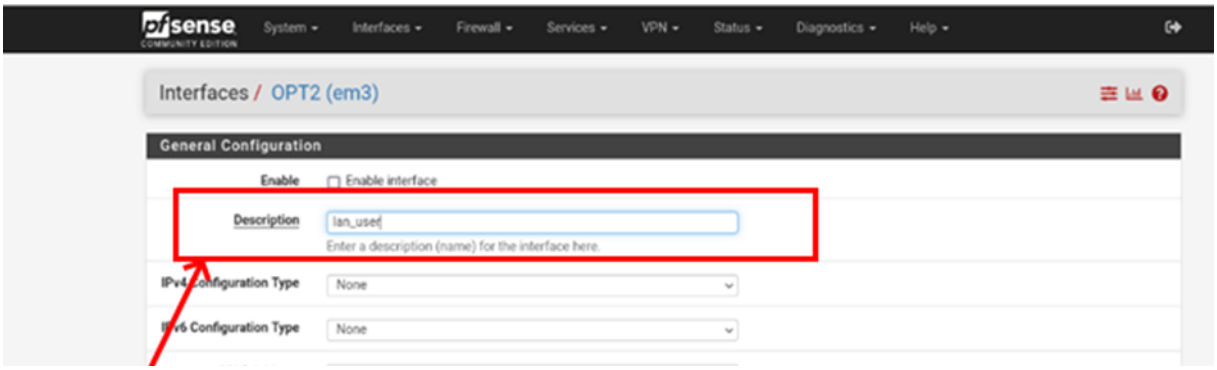
- Cliquer sur l'interface réseau à configurer



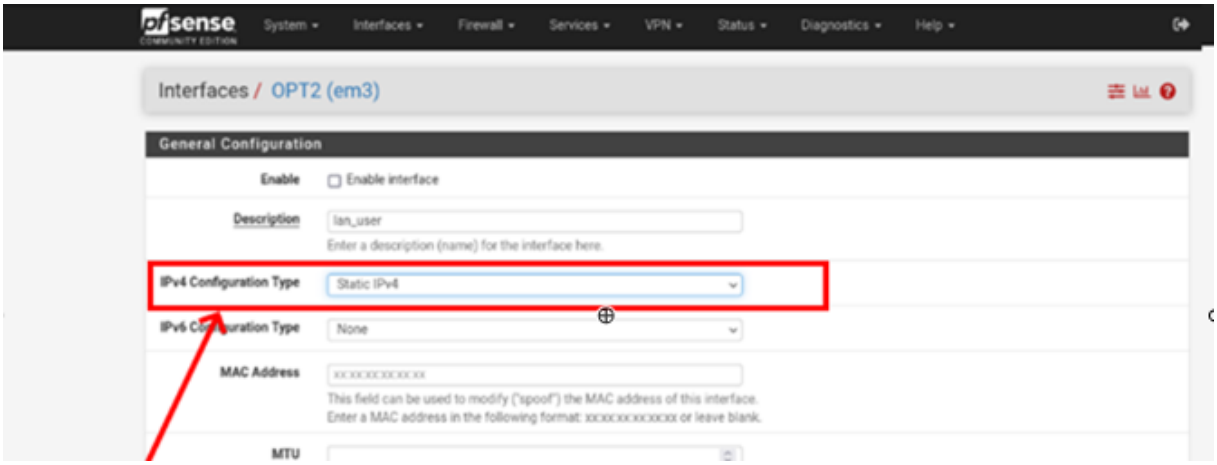
- Cliquer sur « Enable interface » pour activer l'interface réseau.



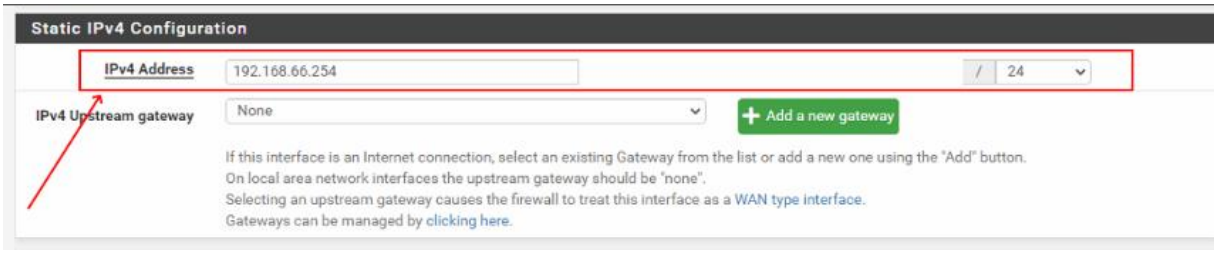
- Mettre dans « Description » le nom du réseau (Par exemple, ici LAN_USER).



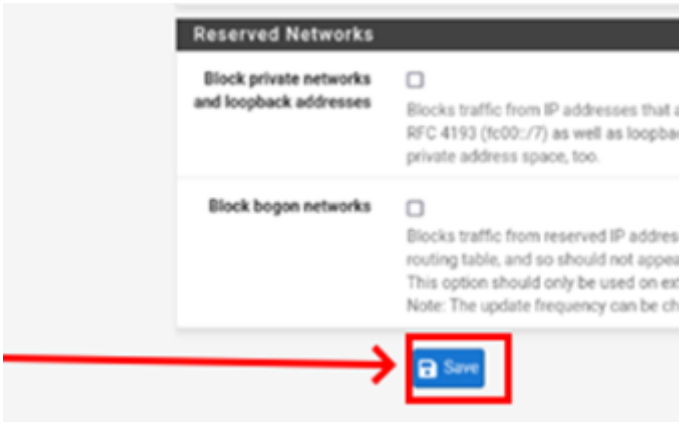
- Dans « IPv4 Configuration Type », mettre en « Static IPv4 ».



- Renseigner l'adresse IP de la passerelle et le masque.



- Cliquer sur Save pour sauvegarder votre configuration de l'interface réseau.



- Cliquer maintenant sur « Apply change » tout en haut de la page pour appliquer les changements.

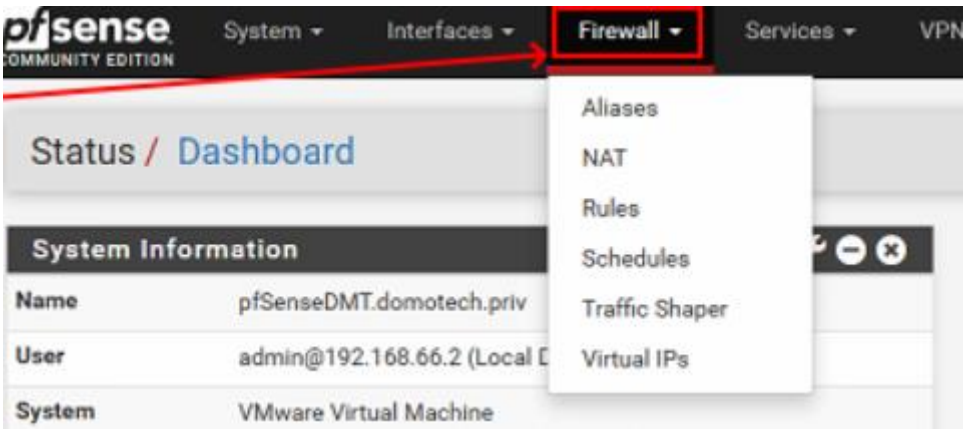
- Réitérer l'opération pour l'ensemble des interfaces réseaux à ajouter.

II) Configuration Outbound

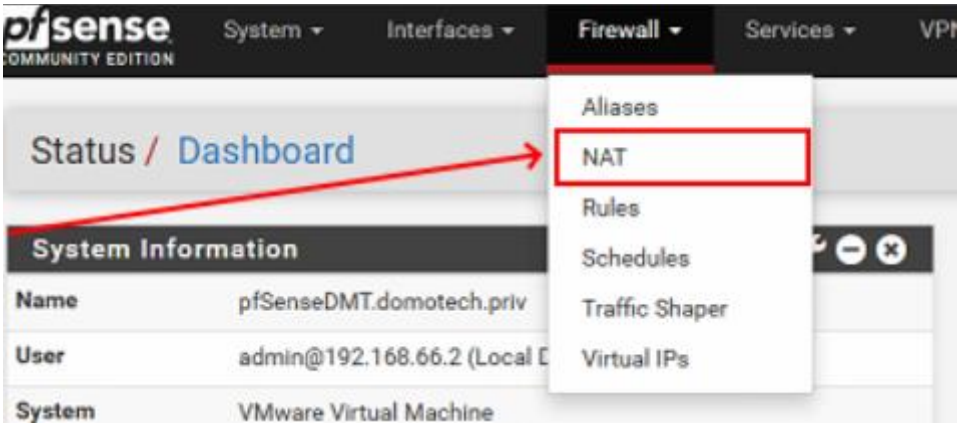
Les Outbound sur pfSense font référence à la configuration des règles de pare-feu sortantes pour les paquets qui quittent le réseau local vers Internet ou un autre réseau distant.

Nous allons configurer la communication entre le LAN SERVER et LAN USER.

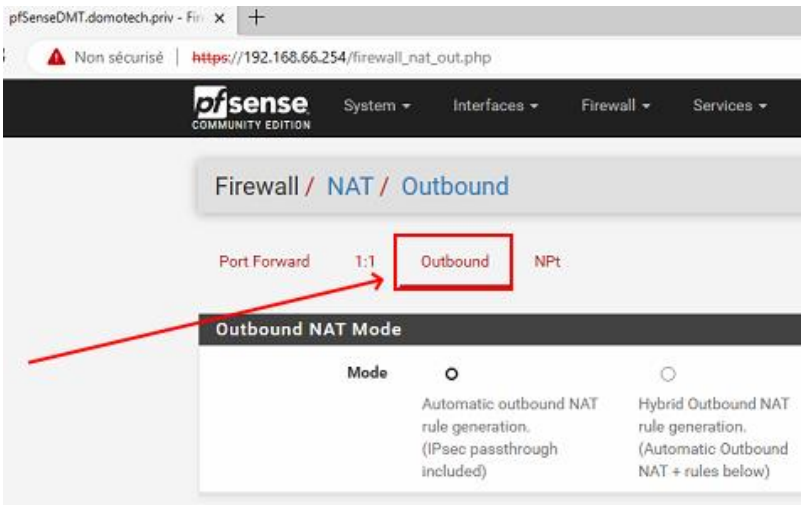
- Cliquer sur « Firewall ».



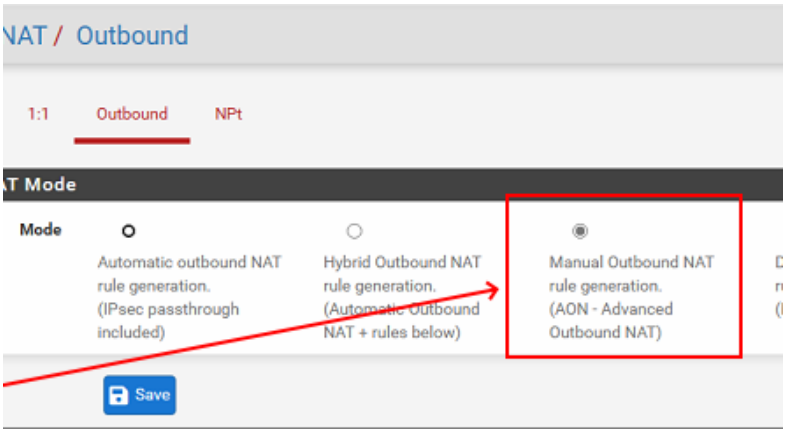
- Cliquer ensuite sur « NAT ».



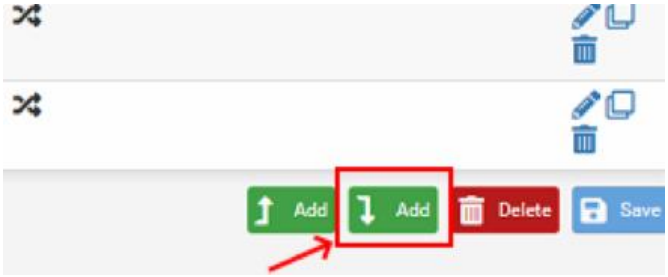
- Cliquer sur « Outbound ».



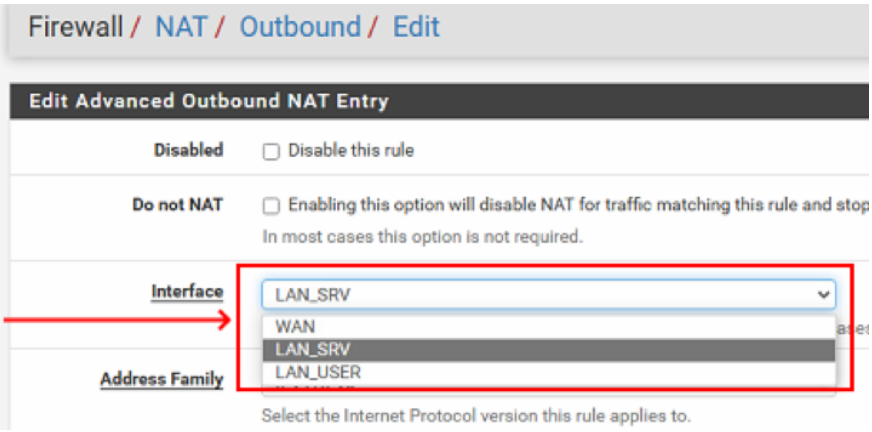
- Cliquer sur le mode « Manual » pour configurer nous-même.



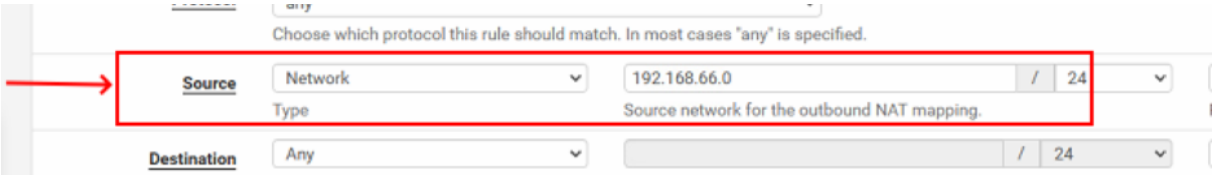
- Cliquer sur « Add » avec une flèche vers le bas pour que ce soit plus lisible



- Choisir le réseau à qui nous voulons donner accès à d'autre réseau (Il s'agit de nos différents LAN USER et SERVER).



- Renseigner l'IP réseau des réseaux que l'on a configurés.



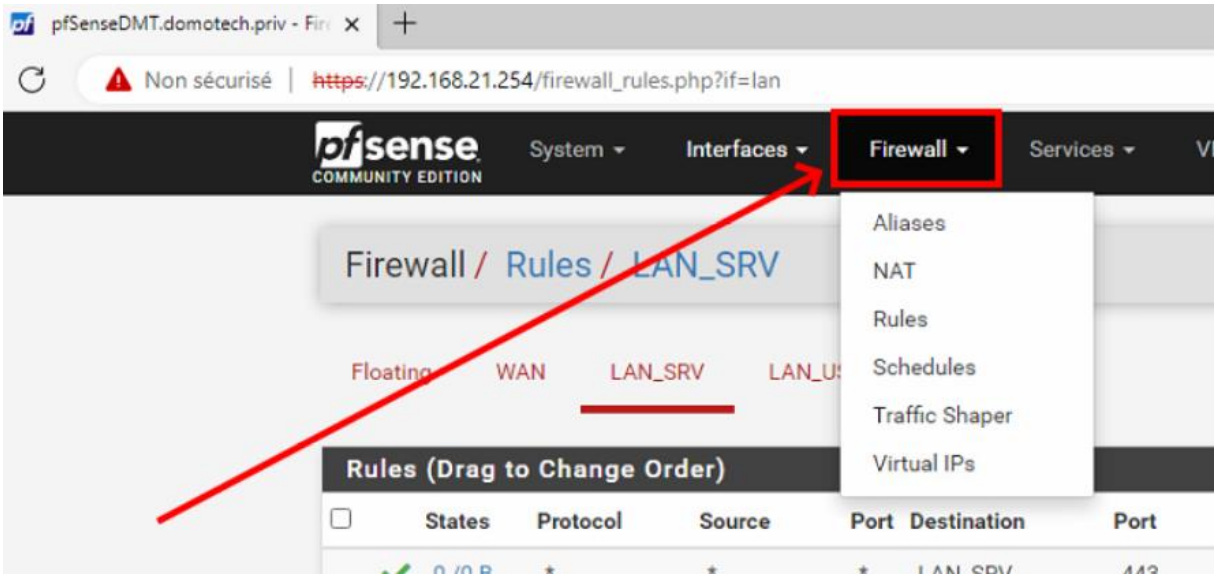
- Cliquer ensuite sur « Save » et créer toutes les entrées que vous voulez

III) Configuration du firewall PFSense

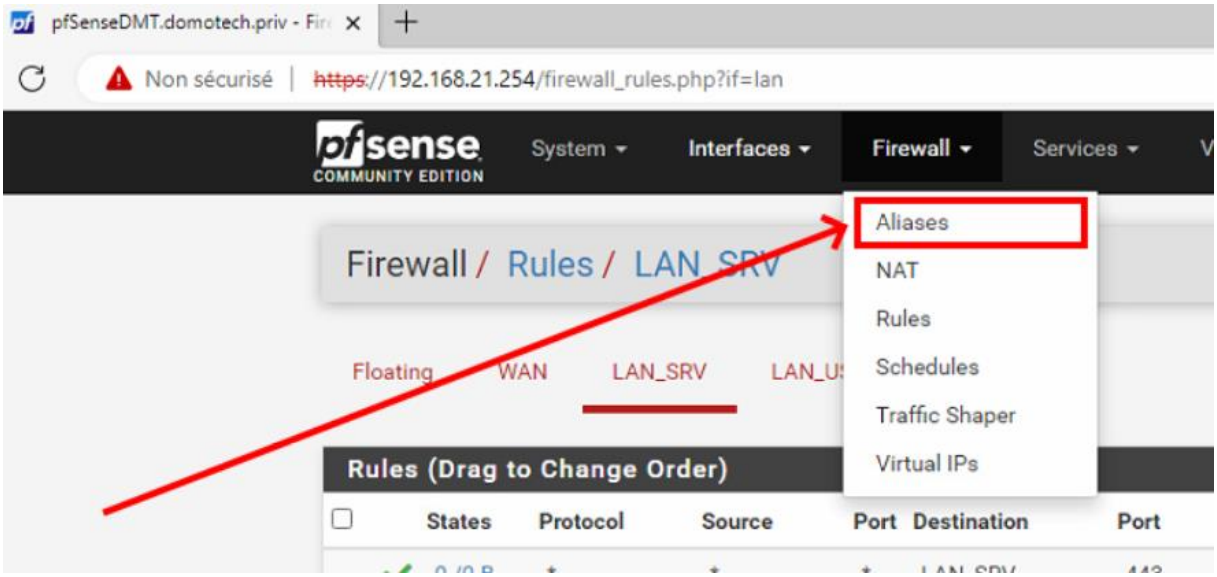
a. Création des Aliases

Les Aliases sont des noms uniques qui permettent de regrouper plusieurs adresses IP, noms et ports afin de simplifier la configuration des règles du pare-feu.

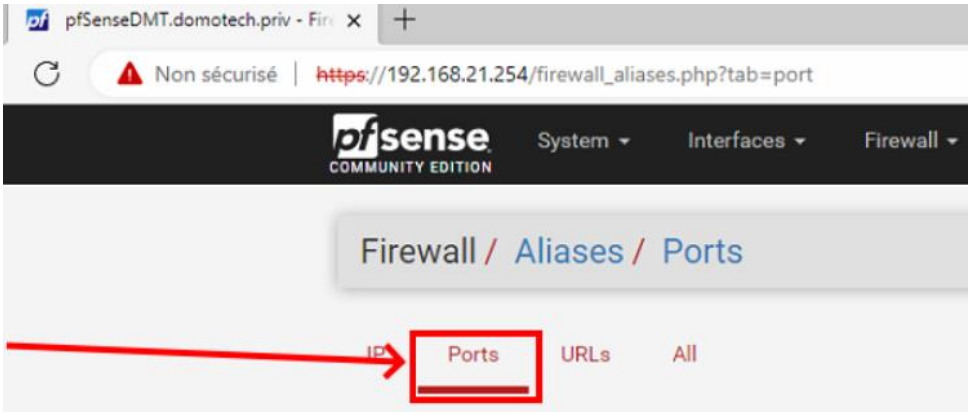
- Cliquer sur « Firewall ».



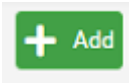
- Cliquer sur « Aliases ».



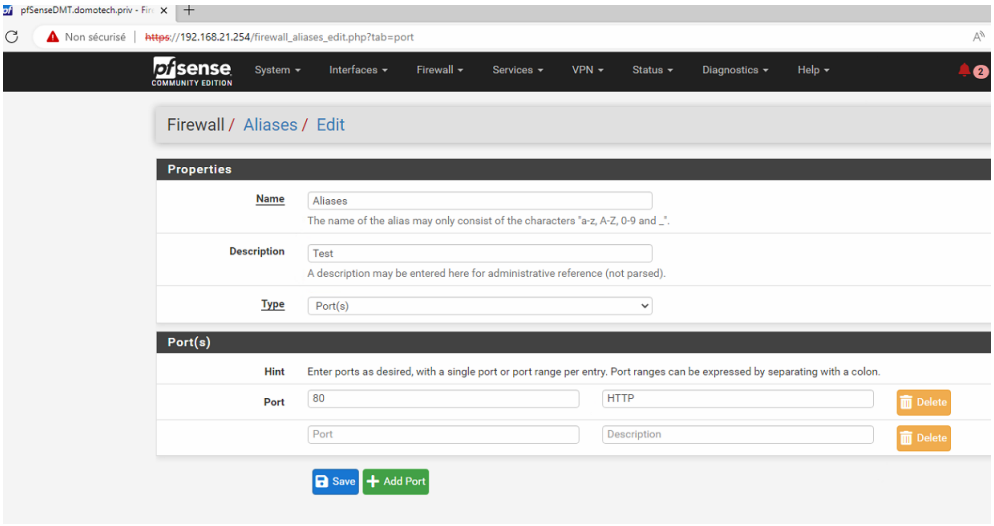
- Cliquer sur « Ports »



- Cliquer sur « + ADD » pour ajouter un aliases.



- Renseigner un nom, une description, le type et les ports à regrouper par exemple. Les aliases peuvent aussi regrouper des noms, et également des IP.



- Dans l'infrastructure de DOMOTech, les aliases suivants ont été créés afin d'être utilisé pour la mise en place de la matrice de flux de services.

Firewall Aliases Ports

Name	Values	Description	Actions
AD	389, 88	Authentification AD	
Browsing	80, 443, 8080, 53	List of Browsing Ports	
File_Transfer	20, 21, 22	Transfert de fichiers	
Mail_Access	143, 993, 110, 995	Accès au courrier	
RemoteMGMT	80, 22, 3389	For management access	

Add Import

b. Règles du pare-feu

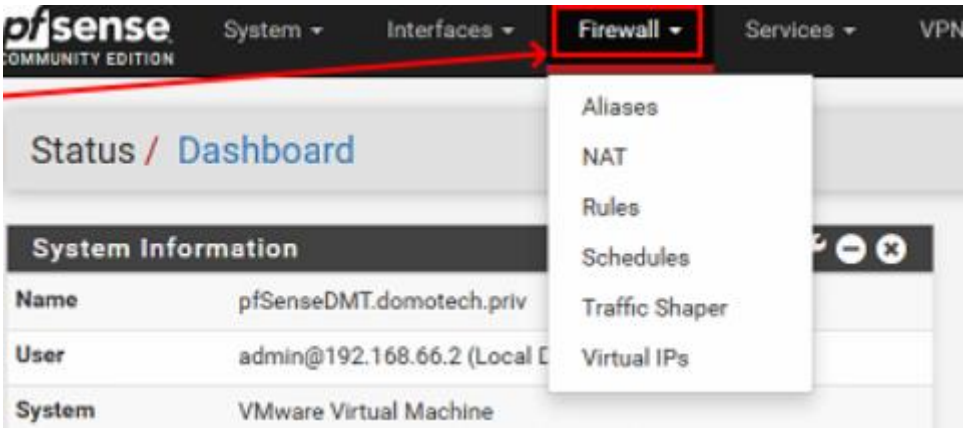
Plusieurs règles ont été mises en place pour sécuriser le réseau de DOMOTech. Ces règles sont présentes dans le document « Matrice de flux des services » **(Annexe 3).**

c. Configuration des règles de pare-feu

Une règle de pare-feu est une instruction ou un ensemble d'instructions qui permet de contrôler le trafic réseau entrant ou sortant d'un système informatique. Le pare-feu analyse chaque paquet de données qui entre ou sort du réseau et décide si le paquet doit être autorisé ou bloqué en fonction des règles de pare-feu configurées. La matrice de flux des services DOMOTech apportent des détails sur les services autorisés.

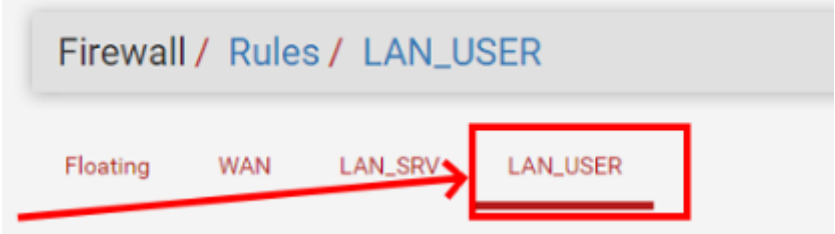
Nous allons configurer la communication entre le LAN SERVER et LAN USER, et le WAN.

- Cliquer sur « Firewall ».

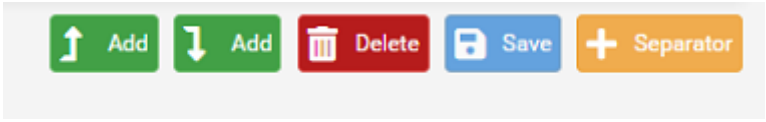


- Cliquer ensuite sur « Rules ».

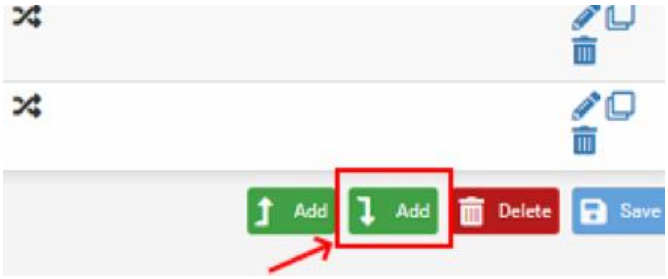
- Cliquer sur un LAN.



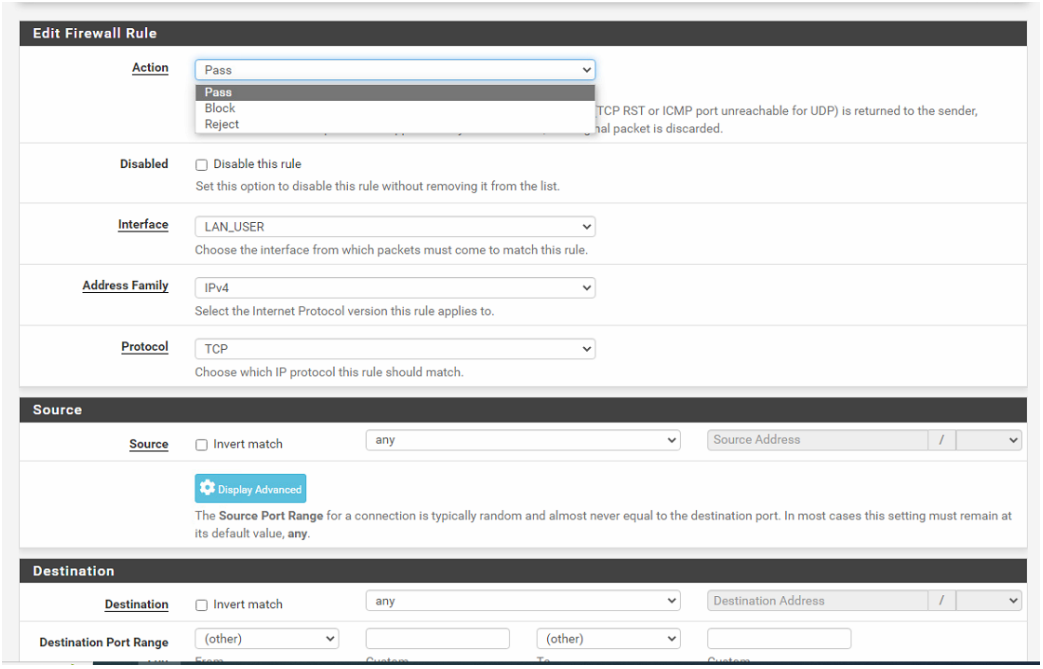
- Les règles fonctionnent en commençant par la plus haute à la plus basse.
  Il est également possible de créer des « separator » afin d'avoir une meilleure visibilité et gestion sur les règles.
  La première règle sera de bloquer toutes les connexions du LAN vers les autres afin de les débloquer en utilisant la matrice.



- Cliquer sur « Add »

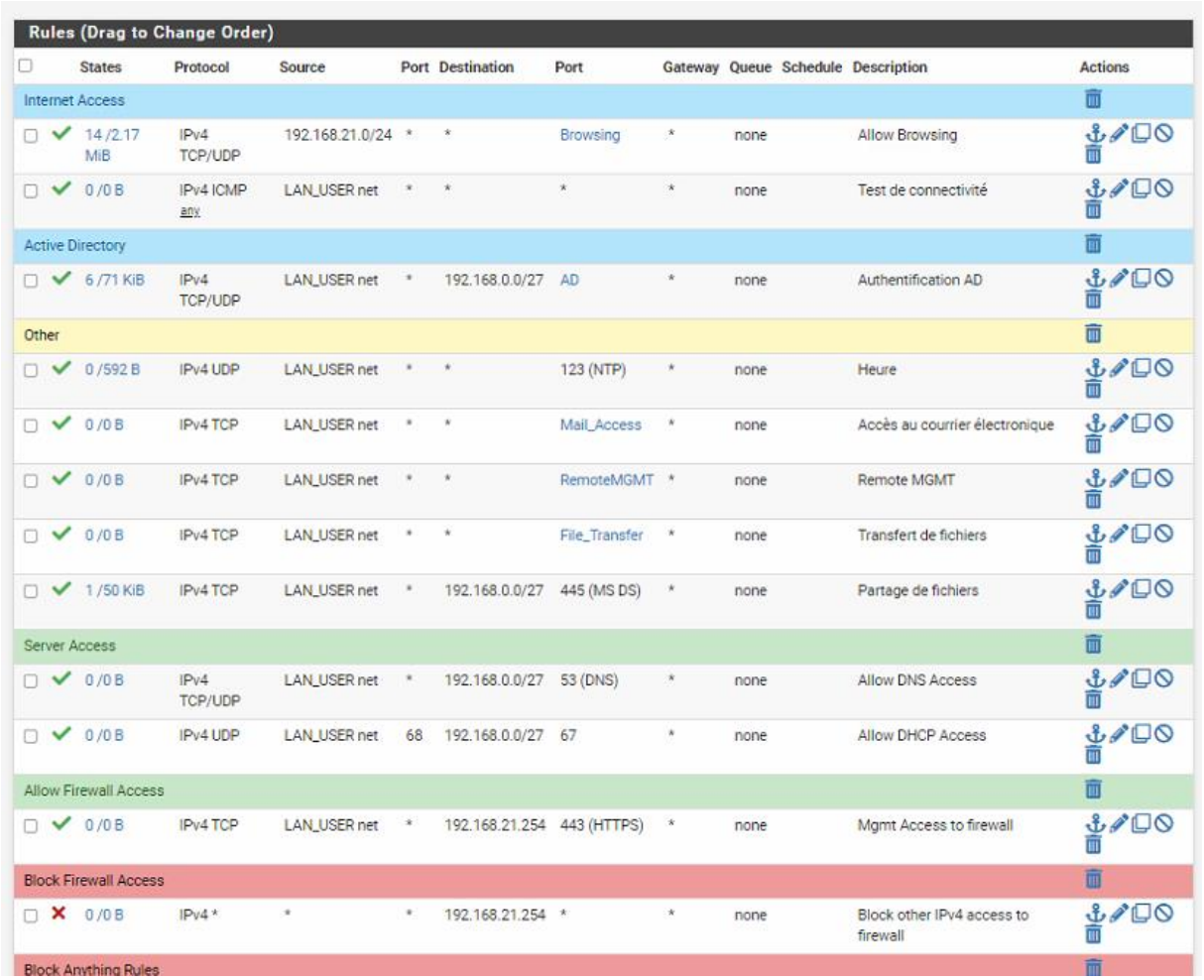


- Pour cette règle,
  - Action : Block
  - Protocol : Any
  - Source : LAN USER NET, Destination : Any



- Cliquer ensuite sur « Save »

- Configurer l'ensemble des autres règles en utilisant la matrice de flux des services et le cahier de test pour vérifier le bon fonctionnement de chaque règle.



Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	Internet Access										
✓	14 /2.17 MiB	IPv4 TCP/UDP	192.168.21.0/24	*	*	Browsing	*	none		Allow Browsing	
✓	0 /0 B	IPv4 ICMP any	LAN_USER net	*	*	*	*	none		Test de connectivité	
	Active Directory										
✓	6 /71 KiB	IPv4 TCP/UDP	LAN_USER net	*	192.168.0.0/27	AD	*	none		Authentification AD	
	Other										
✓	0 /592 B	IPv4 UDP	LAN_USER net	*	*	123 (NTP)	*	none		Heure	
✓	0 /0 B	IPv4 TCP	LAN_USER net	*	*	Mail_Access	*	none		Accès au courrier électronique	
✓	0 /0 B	IPv4 TCP	LAN_USER net	*	*	RemoteMGMT	*	none		Remote MGMT	
✓	0 /0 B	IPv4 TCP	LAN_USER net	*	*	File_Transfer	*	none		Transfert de fichiers	
✓	1 /50 KiB	IPv4 TCP	LAN_USER net	*	192.168.0.0/27	445 (MS DS)	*	none		Partage de fichiers	
	Server Access										
✓	0 /0 B	IPv4 TCP/UDP	LAN_USER net	*	192.168.0.0/27	53 (DNS)	*	none		Allow DNS Access	
✓	0 /0 B	IPv4 UDP	LAN_USER net	68	192.168.0.0/27	67	*	none		Allow DHCP Access	
	Allow Firewall Access										
✓	0 /0 B	IPv4 TCP	LAN_USER net	*	192.168.21.254	443 (HTTPS)	*	none		Mgmt Access to firewall	
	Block Firewall Access										
✗	0 /0 B	IPv4 *	*	*	192.168.21.254	*	*	none		Block other IPv4 access to firewall	
	Block Anything Rules										

Après configuration des règles sur le LAN_USER

IV) Cahier de tests

L'ensemble des tests pour la mise en place de nouvelles règles seront réalisés sur les équipements terminaux.

- DNS : Vérifier la résolution de noms avec nslookup
- HTTP : Tester la connectivité à un site en http
- HTTPS : Tester la connectivité à un site en https
- HTTP PROXY : Faire un speedtest (qui utilise le port 8080)
- LDAP : Vérifier l'authentification avec un compte user et mot de passe
- Kerberos : Vérifier l'authentification avec un compte user et mot de passe
- SMB : Se connecter à un filer
- NTP : Vérifier l'heure système
- ICMP : Réaliser un ping
- RDP : Se connecter à un serveur avec « mstsc.exe »
- SSH : Se connecter à un serveur distant avec « PuTTY.exe »
- FTP : Tester un transfert de fichier FTP
- SFTP : Tester un transfert de fichier SFTP
- RPC : Tester VEEAM
- SMTP : Vérifier l'envoi de courriels via le protocole SMTP depuis un client de messagerie.
- IMAP : Vérifier l'envoi de courriels via le protocole SMTP depuis un client de messagerie.
- IMAPS : Vérifier la récupération de courriels via le protocole IMAPS depuis un client de messagerie.
- POP3 : Vérifier la récupération de courriels via le protocole IMAPS depuis un client de messagerie.
- POP3S : Vérifier l'envoi de courrier électronique chiffré via SMTPS depuis un client de messagerie.

Ce cahier de test donne la liste des tests à effectuer pour les divers protocoles de la matrice de flux et dans les différents sens indiqués par celle-ci.

La première règle bloquant tout, il est important de réaliser le cahier de test en même temps que la configuration des règles. (Troubleshooting)