**RAPPORT DE STAGE**

**Domaine d’études :** Sécurité des Systèmes Informatiques et Réseaux

**Niveau :** 2ème Année

**Sujet :** Administration et Sécurisation d’une Infrastructure Réseau avec pfSense



**Réalisé par :** Ayoub Touihri

**Encadré par :** Mr. Marouane Ben Abdennebi

**Année Universitaire :** 2024/2025

**Reme****rciements**

Je tiens tout d’abord à exprimer ma gratitude envers l'Institut Supérieur des Etudes Technologiques de Radès pour la qualité de sa formation, qui m’a fournit les bases techniques et méthodologiques indispensables à la réussite de ce projet. Mes remerciements s’adressent également aux intervenants professionnels du département des Technologies de l’Information (TI) pour leur engagement à transmettre des savoirs ancrés dans les réalités du terrain.

Une mention toute particulière revient à mon encadrant, Monsieur Marouane Ben Abdennebi, dont l’expertise en sécurité réseau et la pédagogie patiente ont guidé chacune de mes étapes. Merci pour votre disponibilité, vos retours constructifs et votre confiance, surtout lors des défis techniques liés au déploiement de pfSense.

Ce projet a été bien plus qu’une expérience académique : une preuve concrète que la collaboration et la passion sont les clés de la réussite.

**Sommaire**

**Introduction Générale**

**Chapitre 1 : Cadre du stage..........................................................……7 - 12**

1.1 Présentation de la société d’accueil  
 1.1.1 New Technology Services Info : Spécialiste en solutions réseau  
 1.1.2 Environnement technologique (Open Source, virtualisation)  
 1.2 Présentation de l’organisme d’accueil  
 1.2.1 Historique de l’entreprise  
 1.3 Activités principales

1.4 Objectife de stage  
 1.5 Environnement technologique  
 1.6 Méthodologie de travail  
 1.6.1 Étapes clés du projet  
 1.6.2 Outils utilisés

### **Chapitre 2 : Fondements théoriques et concepts clés...........………...13 - 31**

2.1 Concepts clés en réseau et sécurité

2.1.1 VLANs : Isolation et segmentation du réseau avec pfSense

2.1.2 Firewall : Gestion des règles et alias

2.1.3 NAT/PAT et routage inter-VLAN avec le firewall

2.1.4 QoS : Limitation de bande passante par utilisateur

2.1.5 Firewall et filtrage des accès : Théorie et enjeux

2.2 Gestion du réseau

2.2.1 LACP et agrégation de liens pour la redondance et le débit

2.2.2 STP/RSTP/MSTP et limitations dans une topologie dual-switch

2.2.3 Routage statique vs dynamique (OSPF) pour assurer la haute disponibilité

2.3 Présentation de pfSense : Fonctionnalités essentielles

2.3.1 Modules avancés : pfBlockerNG, SquidGuard, Snort

2.4 Virtualisation : Environnement de test

2.4.1 Déploiement de pfSense sous KVM et VMware

2.4.2 Tests et problèmes rencontrés en lab

### **Chapitre 3 : Mise en place des configurations de base........................32 - 42**

3.1 Création du VLAN Administrateurs et segmentation réseau  
 3.1.1 Définition du VLAN Administrateurs dans pfSense  
 3.1.2 Configuration du routage et du filtrage inter-segments pour le VLAN Administrateurs via le firewall

3.2 Configuration DHCP/DNS pour le VLAN Administrateurs  
 3.2.1 Assignation d’adresses IP et serveurs DNS pour le VLAN Administrateurs  
 3.2.2 Choix et configuration entre DNS Forwarder et DNS Resolver pour le VLAN Administrateurs  
 3.2.3 Gestion des résolutions DNS avec Unbound et blocage des DNS externes pour le VLAN Administrateurs

3.3 Vérifications et tests de connectivité

3.3.1 Validation de l’attribution des adresses DHCP

3.3.2 Utilisation de l'outil de diagnostic

3.3.3 Analyse des logs système

### **Chapitre 4 : Mise en œuvre du filtrage avec pfSense............................43 - 52**

4.1. Filtrage des sites web et restrictions d’accès

  4.1.1. Blocage par règles et alias

  4.1.2. Filtrage par Domain Override en DNS

  4.1.3. Filtrage avancé avec pfBlockerNG et planification (schedules)

4.2. Gestion des accès selon un planning et pfBlockerNG

  4.2.1 Planification des blocages selon les horaire

4.2.2 Filtrage avancé avec pfBlockerNG et planification (schedules)

### **Chapitre 5 : Application en environnement réel....................................53 - 57**

5.1. Filtrage par règles et alias

 5.1.1. Résultats et efficacité du blocage par règles et alias

 5.1.2. Problèmes rencontrés et solutions pour éviter les échecs

5.2. Filtrage par Domain Override en DNS

 5.2.1. Évaluation du fonctionnement de la redirection DNS

 5.2.2. Difficultés constatées et stratégies pour les contourner

5.3. Filtrage avancé avec pfBlockerNG et planification (schedules)

 5.3.1. Analyse des résultats de pfBlockerNG appliqué aux VLANs

#### **Conclusion Générale**

#### **Bibliographie/Webographie**

1. **VMware**, "Network Address Translation", [en ligne], 2025,<https://www.vmware.com/topics/network-address-translation> .
2. **YU, Laura**, "How to Configure Inter-VLAN Routing on Layer 3 Switches", *Medium*, 2023,<https://medium.com/@laurayu_653/how-to-configure-inter-vlan-routing-on-layer-3-switches-8c30156a460a> .
3. **Citrix**, "Configuring Link Aggregation", *Citrix Docs*, 2024,<https://docs.netscaler.com/en-us/citrix-adc/current-release/networking/interfaces/configuring-link-aggregation.html> .
4. **GOFFINET, Simon**, "Spanning Tree (STP, RSTP, PVST+)", *Cisco Goffinet*, 2023,<https://cisco.goffinet.org/ccna/redondance-de-liens/spanning-tree-rapid-stp-pvst-cisco/> .
5. **TechTarget**, "OSPF (Open Shortest Path First)", *SearchNetworking*, 2024,<https://www.techtarget.com/searchnetworking/definition/OSPF-Open-Shortest-Path-First> .

#### **Annexes**

KVM et virt-manager setup

pfsense Setup

Pour assurer la Vérification, les architectures, schémas, scripts et configurations sont disponibles sur mon dépôt GitHub:

Lien : <https://github.com/21Yeet21/StageL2RSI.git>

Ce dépôt contient notamment :

- Les architectures initiales du réseau (versions conceptuelles).

- Les schémas et architectures finaux créés .

- Les configurations pfSense exportées (fichiers XML).

- Les figures créées ou modifiées pour ce rapport.

La liste de toutes les figures présentes dans ton rapport :

Figure 0 : Architecture générale du réseau cible (première version)

Figure 1 : Exemple de création d’un VLAN dans pfSense

Figure 2 : Exemple d’application d'adresse pour le VLAN Guest

Figure 3 : Création d’un alias pour le VLAN Technicien dans pfSense

Figure 4 : Liste des alias pour les VLANs

Figure 5 : Schéma expliquant le NAT

Figure 6 : Routage inter-VLAN via un switch L3

Figure 7 : Création d’un limiteur de bande passante à 10 Mbps

Figure 8 : Sélection d’alias du VLAN Guest et tous les protocoles

Figure 9 : Application des limiteurs dans la règle + résultat

Figure 10 : Création de règle de pare-feu pour tout accès entrant au service HTTPS (Port 443) sous VLAN Travailleurs depuis le WAN + résultat

Figure 11 : Schéma d’agrégation de liens LACP entre des switches

Figure 12 : Utilisation de MSTP (Spanning Tree) pour améliorer la résilience dans une infrastructure

Figure 13 : Comparaison des protocoles BGP et OSPF pour la redondance et la connectivité

Figure 14 : Installation de pfBlockerNG

Figure 15 : Installation de pfSense sous KVM, voir annexes pour plus de détails

Figure 16 : Ordre incorrect des règles

Figure 17 : Ordre correct des règles

Figure 18 : Création du VLAN Recherche dans pfSense

Figure 19 : Architecture générale du réseau cible (version finale)

Figure 20 : Création d’un alias pour grouper tous les VLANs internes

Figure 21 : Configuration d’une règle de pare-feu pour le VLAN Recherche permettant l'accès à tous les VLANs internes

Figure 21’ : Configuration d’une règle de pare-feu pour bloquer l'accès depuis tous les VLANs internes vers VLAN Recherche + résultat

Figure 22 : Configuration DHCP pour le VLAN Recherche (Services > DHCP > ServerRECH)

Figure 23 : Configuration du DNS Resolver avec activation de DNSSEC et SSL/TLS dans pfSense

Figure 24 : Configuration du DNS Resolver (Unbound) dans pfSense

Figure 25 : Baux DHCP attribués dans pfSense et dans une machine du VLAN Recherche

Figure 26 : Test Ping depuis le VLAN Recherche vers 8.8.8.8

Figure 27 : Logs système dans pfSense (SysLogs Général)

Figure 28 : Création d'alias des sites à bloquer

Figure 29 : Configuration du blocage par règles et alias dans pfSense

Figure 30 : Configuration du Domain Override dans l’interface DNS vers une adresse non routable

Figure 31 : Interface de configuration des schedules dans pfBlockerNG

Figure 32 : Interface générale de pfBlockerNG (Firewall > pfBlockerNG)

Figure 33 : Configuration des règles Inbound et Outbound dans pfBlockerNG

Figure 34 : Attribution des ASN sous le pare-feu pfBlockerNG

Figure 35 : Configuration des paramètres de filtrage dans pfBlockerNG

Figure 36 : Exécution de la mise à jour des listes dans pfBlockerNG

Figure 37 : Règle de pare-feu avant configuration

Figure 38 : Configuration de la règle avec l’alias VLAN\_Internes

Figure 39 : Configuration du planning (Schedule)

Figure 40 : Règle de pare-feu après configuration

Figure 41 : Blocage avec succès pour Instagram

Figure 42 : Blocage échoué pour Facebook

Figure 43 : Blocage avec succès pour Facebook (par Domain Override en DNS)

Figure 44 : Création d’une règle sur le firewall pour bloquer le trafic vers un serveur DNS externe

Figure 45 : Blocage avec succès pour Facebook (avec pfBlockerNG)

#### **Introduction**

La société **New Technology Services Info**, fondée en 2018 et située à Ezzahra, opère dans les domaines de la technologie, des réseaux, et de l'ingénierie. Spécialisée dans les solutions réseau, cette entreprise se distingue par ses services innovants et adaptés aux besoins des entreprises locales.

J’ai choisi d’effectuer mon stage de perfectionnement au sein de cette entreprise en raison de la pertinence de ses solutions réseau, qui sont directement en lien avec mon domaine d’études. En tant qu’étudiant spécialisé dans les réseaux, cette opportunité représente une occasion idéale pour approfondir mes connaissances et développer des compétences pratiques.

Mon objectif principal pour ce stage est de me perfectionner dans l’administration d’une infrastructure réseau, en particulier à travers l’utilisation du pare-feu pfSense, un choix pertinent dans la sécurisation et la gestion des réseaux modernes.

# **Chapitre 1 : Cadre du stage**

## **1.1 Présentation de la société d’accueil**

### **1.1.1 New Technology Services Info : Spécialiste en solutions réseau**

Fondée en 2018 et située à Ezzahra, **New Technology Services Info (NTS)** est une entreprise spécialisée dans la conception et la mise en œuvre de solutions réseau modernes et sécurisées.

Son objectif principal est d’accompagner les entreprises dans l’optimisation et la sécurisation de leurs infrastructures informatiques. L’entreprise se distingue par ses domaines d’expertise suivants :

* **Administration réseau** : mise en place de solutions fiables et performantes pour garantir une connectivité optimale.
* **Sécurité informatique** : déploiement de pare-feu et de systèmes de détection d’intrusions.
* **Support technique** : accompagnement et résolution des problématiques informatiques des clients.

### **1.1.2 Environnement technologique (Open Source, virtualisation)**

### NTS repose sur des outils technologiques modernes et efficaces, principalement issus du monde open source :

* **pfSense** : pare-feu avancé pour la gestion et la sécurisation des réseaux.
* **KVM (Kernel-based Virtual Machine)** : virtualisation pour optimiser l’utilisation des serveurs.
* **AlmaLinux** : système d’exploitation open source reconnu pour sa stabilité et ses performances.
* **OpenVPN** : solution de sécurisation des connexions à distance.

Cet environnement technologique permet à NTS de fournir des solutions sur mesure, économiques et adaptées aux besoins de chaque client.

## **1.2 Présentation de l’organisme d’accueil**

### **1.2.1 Historique de l’entreprise**

### Depuis sa fondation en 2018, New Technology Services Info (NTS) s’est imposée comme un acteur clé dans le domaine des technologies de l’information, en offrant des services novateurs et sécurisés pour répondre aux besoins croissants des entreprises en matière de réseaux.

### **1.3 Activités principales**

## Les activités de NTS incluent :

Administration et gestion d’infrastructures réseau.

Déploiement de solutions de sécurité basées sur des technologies open source.

Conseil et assistance technique pour la maintenance et la configuration des systèmes informatiques.

### **1.4 Environnement technologique**

## Pour répondre aux besoins variés de ses clients, NTS utilise les technologies suivantes :

* **pfSense** pour le contrôle et la gestion des réseaux.
* **KVM** pour la virtualisation et l’optimisation des ressources matérielles.
* **AlmaLinux** comme système d’exploitation principal dans ses environnements de production.

Dans le cadre de mon stage chez New Technology Services Info (NTS), une problématique a été définie conjointement avec mon encadrant afin de simuler un projet concret et adapté à une infrastructure réelle. Cette problématique repose sur l’idée suivante :

La mise en place d’un réseau d’entreprise composé de trois blocs distincts a la première place puis un autre bloc serait ajouter , avec la possibilité d’établir des règles d’isolation ou de communication entre eux, selon les besoins.

La centralisation de l’administration et de la supervision des règles de sécurité via un pare-feu pfSense pour garantir une gestion simplifiée et efficace.

Le contrôle des accès internet par le biais d’un filtrage des sites web, afin de bloquer les plateformes non professionnelles et optimiser l’utilisation des ressources réseau.

## **1.5 Objectifs du stage**

## Mon stage vise à répondre aux problématiques identifiées en réalisant les objectifs suivants :

**Administration réseau** :

Installer et configurer **pfSense** comme pare-feu principal.

Mettre en place des règles pour bloquer les sites web non professionnels.

**Sécurisation des connexions** :

Garantir un réseau sécurisé et supervisé pour protéger les données échangées.

**Supervision et contrôle** :

Surveiller en temps réel le trafic réseau et gérer les utilisateurs.

## **1.6 Méthodologie de travail**

### **1.6.1 Étapes clés du projet**

**Analyse des besoins** :

Audit de l’infrastructure actuelle des trois blocs.

Identification des restrictions nécessaires (ex. filtrage des sites).

**Déploiement technique** :

Installation de **pfSense** et configuration des règles de filtrage.

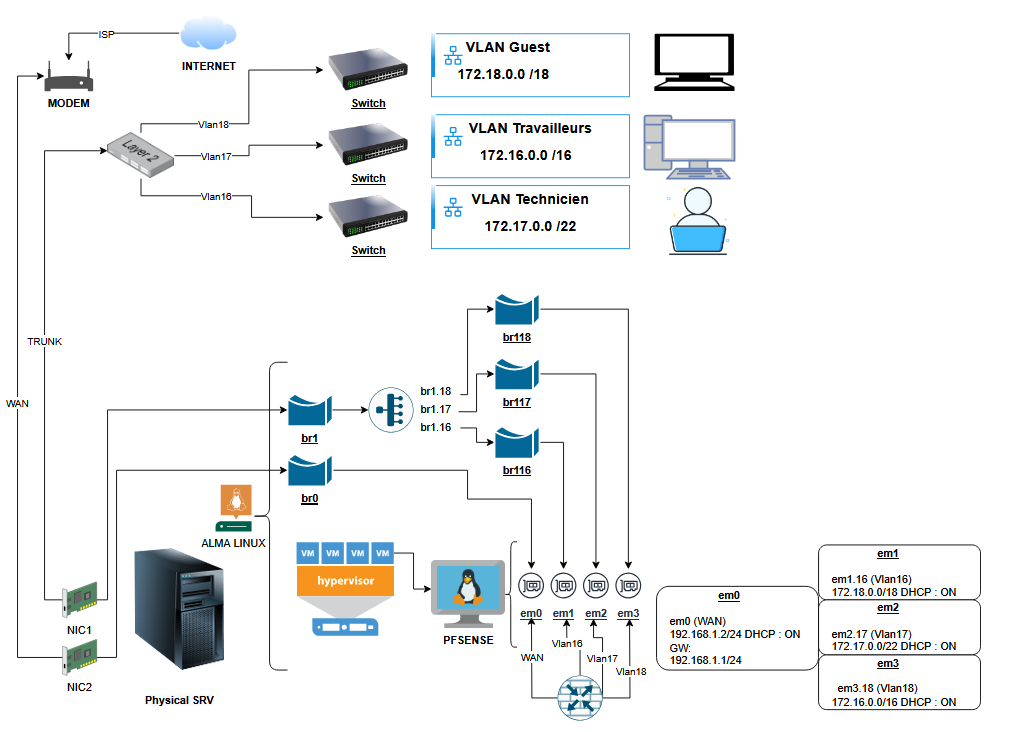
**Tests et validation** :

Simulation de scénarios pour vérifier le fonctionnement du filtrage et des règles réseau.

Ajustements basés sur les résultats des tests pour améliorer la performance et la sécurité.

### **1.6.2 Outils utilisés**

**pfSense** : pare-feu pour la gestion et la sécurisation du réseau et filtrage pour bloquer les sites web non autorisés.



**Figure 0:** Architecture générale du réseau cible (première version)

# **Chapitre 2 : Fondements théoriques et concepts clés**

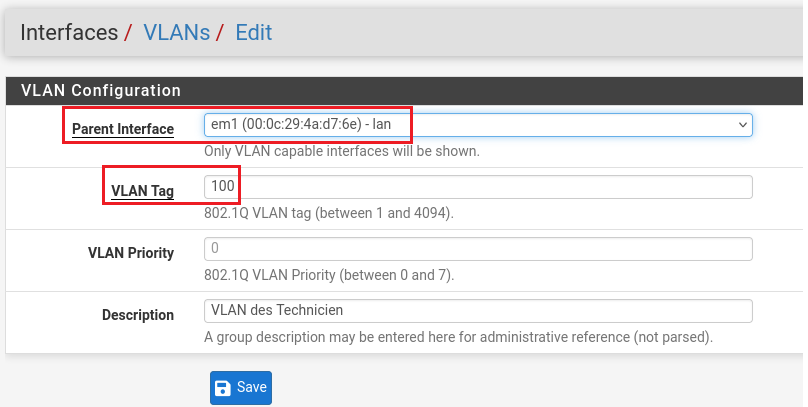
## 

## **2.1 Concepts clés en réseau et sécurité**

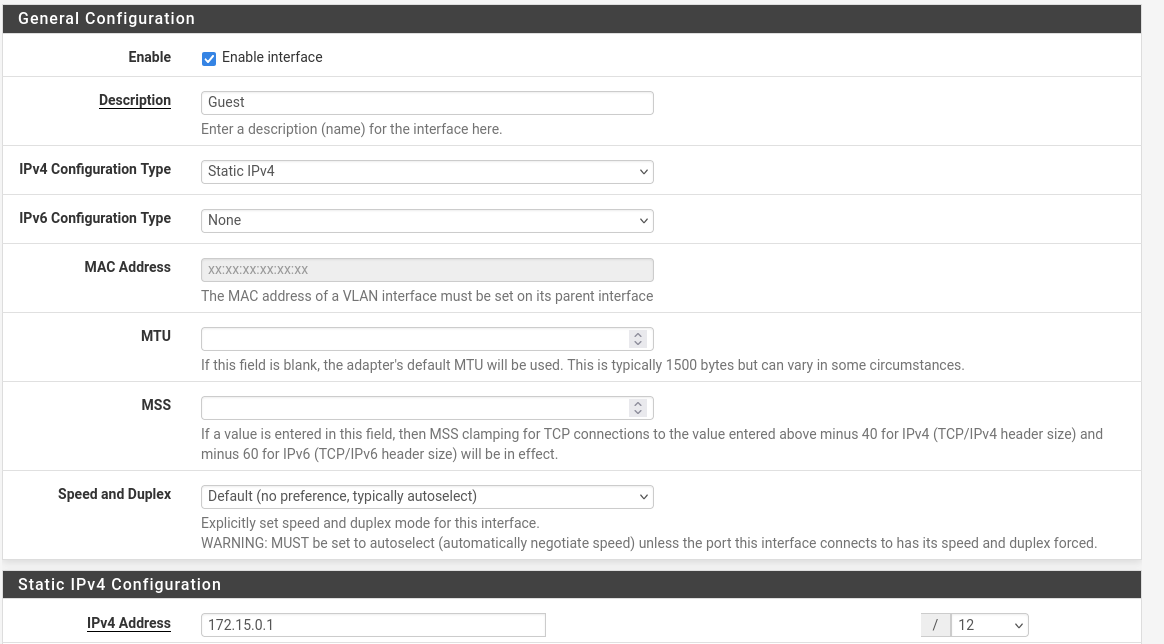
### **2.1.1 VLANs : Isolation et segmentation du réseau avec pfSense**

### Les VLANs (Virtual Local Area Networks) permettent de créer des sous-réseaux logiques au sein d’un même réseau physique. Cette segmentation du réseau permet une gestion plus fine du trafic et renforce la sécurité en isolant les différents services ou départements d’une organisation. Grâce à la norme **802.1Q**, les trames réseau sont marquées avec des tags qui permettent aux commutateurs de diriger le trafic vers les ports appropriés. Cette isolation est cruciale pour limiter la propagation des attaques internes, telles que le sniffing ou le spoofing.

Dans pfSense, la configuration des VLANs est essentielle si on utilise pfsense au lieu du switch L3 pour segmenter le réseau en fonction des besoins de l’organisation, comme l’isolation du département Techniciens ou Travailleur, améliorant ainsi la sécurité et les performances.



**Figure 1:**Exemple de Création d’un VLAN dans pfSense.

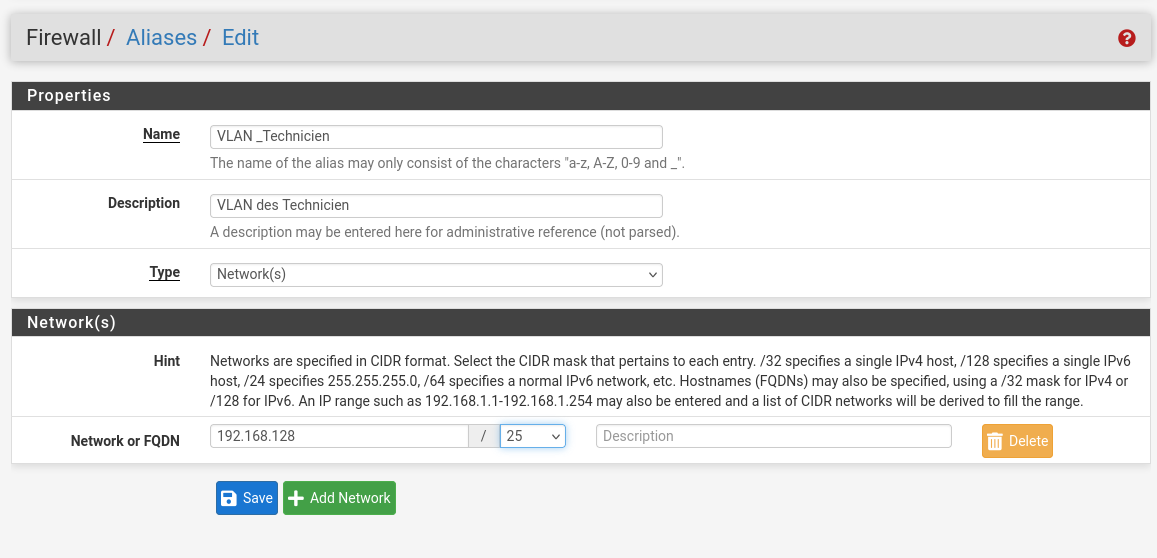


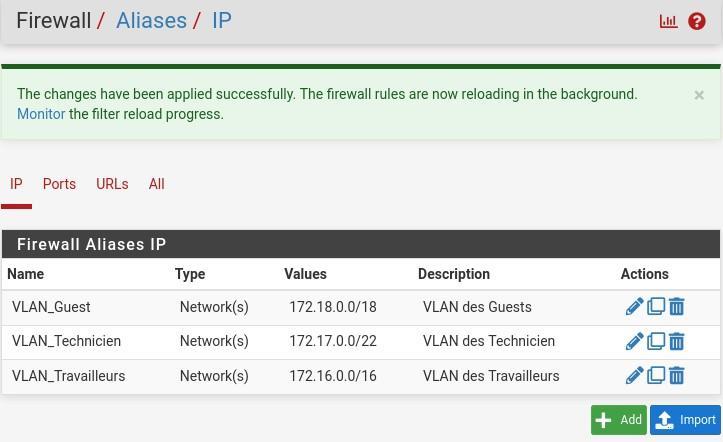
**Figure 2:** Exemple d’Application d'adresse pour le VLAN Guest

### **2.1.2 Firewall : Gestion des règles et alias**

Le pare-feu pfSense permet une gestion détaillée des règles de filtrage du trafic. Les règles sont définies en fonction de critères comme l’adresse IP, les ports et les protocoles. De plus, les alias permettent de regrouper plusieurs adresses, ports ou réseaux sous un même nom, simplifiant la gestion des règles complexes. Cela permet de centraliser la configuration et de maintenir un contrôle optimal sur le trafic réseau.

* Dans la première phase de notre projet, supposons que les VLANs sont déjà créés. Nous commencerons à utiliser des alias pour la gestion des accès et des filtrages dans pfSense. Cela nous permettra de simplifier la configuration tout en conservant un contrôle précis sur le trafic réseau. Plus tard, nous discuterons de l'ajout d'un VLAN supplémentaire, que nous intégrerons à ce moment-là.

****

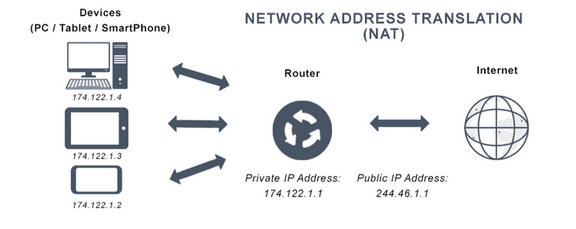
**Figure 3:**Création d’un Alias pour le VLAN Technicien dans pfSense

**Figure 4:**Liste des Aliases pour les VLAN

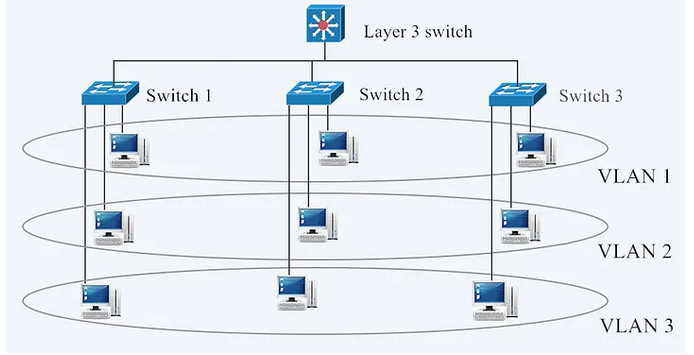
### **2.1.3 NAT/PAT et routage inter-VLAN avec le firewall**

Le NAT (Network Address Translation) et le PAT (Port Address Translation) sont des techniques utilisées pour masquer les adresses IP privées des équipements internes lors de leur communication avec l’extérieur. Ces mécanismes préservent la confidentialité et la sécurité du réseau interne. Le NAT permet de mapper plusieurs adresses privées sur une seule adresse publique, tandis que le PAT associe plusieurs connexions internes à un seul port extérieur.

Le routage inter-VLAN permet à différents VLANs de communiquer entre eux. Cependant, pour maintenir la sécurité, il est crucial de configurer des règles de filtrage appropriées dans le pare-feu pfSense pour contrôler les flux de données entre ces VLANs.



**Figure 5:** Schéma expliquant Le NAT



**Figure 6 :** *Routage inter-VLAN via un switch L3*

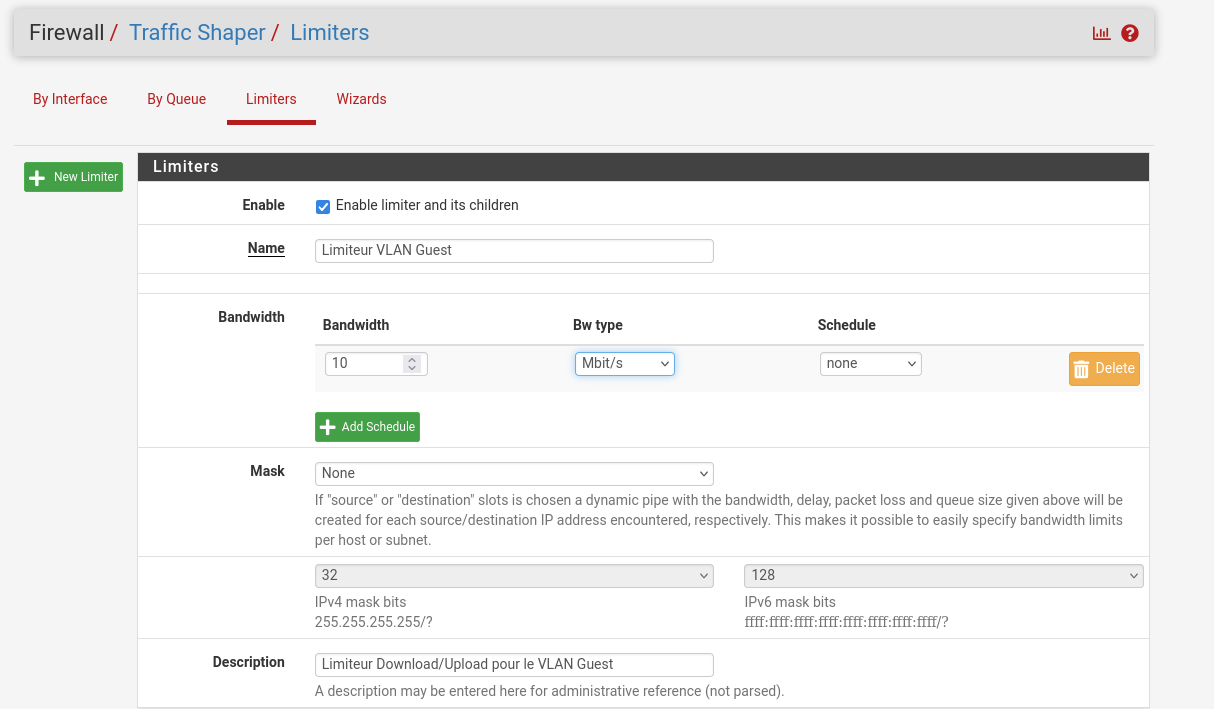
### 

### 

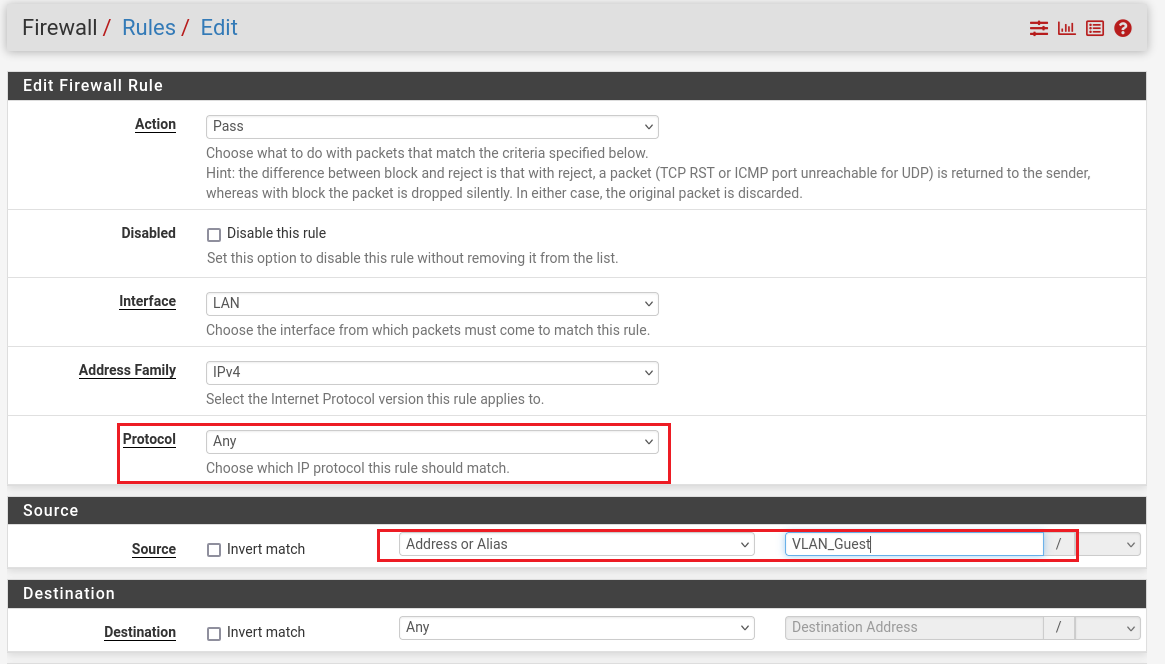
### **2.1.4 QoS : Limitation de bande passante par utilisateur**

La Qualité de Service (QoS) est une technique permettant de gérer la répartition de la bande passante entre les utilisateurs et les applications en fonction de leur priorité. Dans des environnements où la bande passante est limitée, la QoS est essentielle pour garantir que des applications critiques, telles que la VoIP ou le streaming vidéo, bénéficient d’une bande passante suffisante.

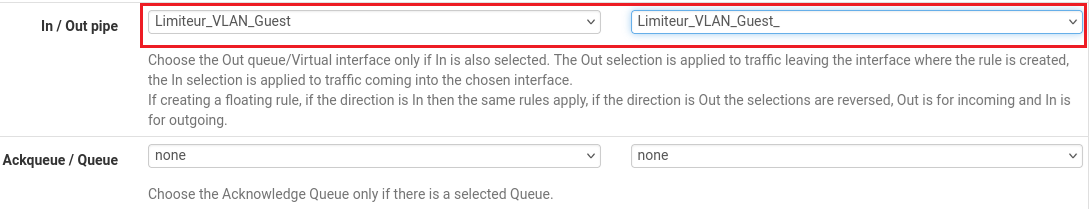
Dans pfSense, la gestion de la QoS se fait à travers le module Traffic Shaper, qui permet de configurer des files d’attente hiérarchiques et de prioriser certains types de trafic. Cela permet de garantir une répartition équitable des ressources réseau tout en optimisant les performances globales.



**Figure 7:** Création d’une Limiteur de la bande passante à 10 Mbps



**Figure 8:** Sélection d’alias du VLAN Guest et tous les Protocol



****

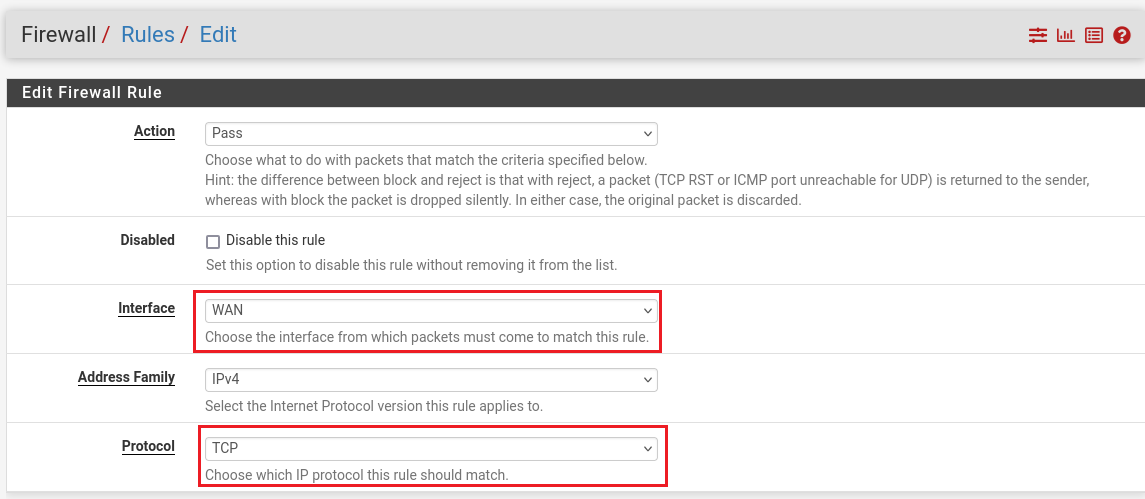
**Figure 9:** Application des Limiteurs dans la règle + résultat

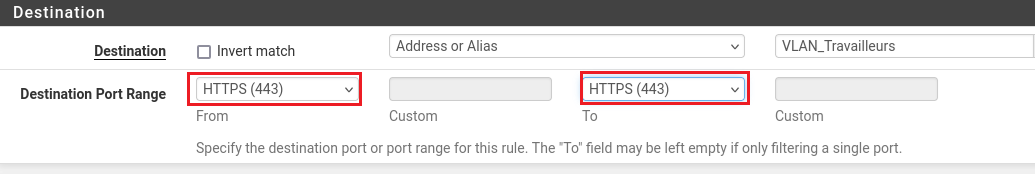
### **2.1.5 Firewall et filtrage des accès : Théorie et enjeux**

Le pare-feu est un composant essentiel pour la sécurité du réseau. Il permet de filtrer le trafic entrant et sortant en fonction de critères comme l’adresse IP, le port ou le protocole. Dans pfSense, les règles du pare-feu sont définies pour autoriser ou bloquer certains types de trafic selon les besoins du réseau.

Les pare-feux jouent un rôle crucial dans la prévention des intrusions et dans la gestion des accès aux ressources réseau. Une configuration incorrecte des règles de filtrage peut exposer l’infrastructure à des risques de sécurité.

* Supposons qu'un serveur HTTPS soit hébergé dans le réseau, situé dans le VLAN des Travailleurs. Pour permettre aux utilisateurs externes d'accéder à ce serveur via Internet, il est nécessaire de configurer une règle dans pfSense pour autoriser le trafic entrant sur le port 443 (HTTPS) depuis l'interface WAN.
* le Protocol est TCP car le HTTPS utilise TCP







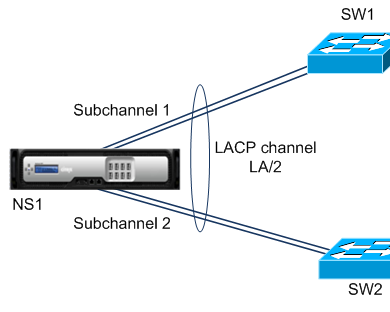
**Figure 10:** Création de règle de Pare-feu pour Tout Accès Entrant au Service HTTPS(Port 443) sous VLAN Travailleurs depuis le WAN + résultat

## **2.2 Gestion du réseau**

### **2.2.1 LACP et agrégation de liens pour la redondance et le débit**

Le **LACP** (Link Aggregation Control Protocol) permet de combiner plusieurs connexions physiques en une seule liaison logique. Cela permet non seulement d'augmenter le débit global mais aussi d’assurer une redondance, ce qui est crucial pour garantir la haute disponibilité du réseau. L’ Agréger des liens permet aussi de répartir la charge sur plusieurs connexions, améliorant ainsi la performance du réseau dans les environnements critiques.

Dans pfSense, la configuration du LACP se fait via l'interface **LAGG** .



**Figure 11:** Schéma d’agrégation de liens LACP entres des Switches

#### 

### **2.2.2 STP/RSTP/MSTP et limitations dans une topologie dual-switch**

Les protocoles STP, RSTP et MSTP empêchent les boucles réseau en désactivant certains chemins redondants. RSTP accélère la convergence, et MSTP gère plusieurs instances de STP, utile pour les réseaux avec VLANs. Toutefois, dans une topologie dual-switch avec commutateurs de niveau 3 (Layer 3), ces protocoles présentent des limites.

### **Limitations de STP/RSTP/MSTP dans une topologie dual-switch**

* Redondance active-active impossible : STP bloque certains liens, laissant un switch en veille.
* Conflits avec LACP en mode Layer 3 : LACP peut créer des déséquilibres si les chemins ne sont pas bien rouverts.
* Basculement lent : STP met du temps à réactiver les liens en cas de panne.

### **Alternative avec des protocoles de routage dynamique**

Pour une redondance active-active, il est préférable d’utiliser des protocoles de routage dynamique comme **OSPF ou BGP** qui permettent :

* Un équilibrage de charge efficace.
* Une réaction rapide aux pannes.
* L’élimination des boucles Layer 2 en favorisant le routage.
* Une meilleure gestion des VLANs routés.



**Figure 12:** Utilisation de MSTP (Spanning Tree) pour améliorer la résilience dans une infrastructure.



**Figure 13:** Comparaison des Protocoles BGP et OSPF pour la Redondance et la Connectivité

### **2.2.3 Routage statique vs dynamique (OSPF) pour assurer la haute disponibilité**

Le routage statique implique la configuration manuelle des routes, adapté aux petits réseaux, mais manque de flexibilité. Le routage dynamique, comme OSPF, s'adapte automatiquement aux changements de topologie et est essentiel pour les réseaux complexes, permettant de trouver le chemin le plus court et de réagir aux pannes.

| **Caractéristique** | **Routage Statique** | **Routage Dynamique (OSPF)** |
| --- | --- | --- |
| **Configuration** | Configuration manuelle des routes. | Configuration automatique via échange de protocoles (paquets Hello, LSAs). |
| **Flexibilité** | Peu flexible : ne s’adapte pas aux changements de topologie. | Très flexible : recalcule automatiquement les chemins en cas de panne ou de modification. |
| **Adaptabilité aux pannes** | Aucune réaction aux pannes: nécessite une intervention manuelle. | Réaction immédiate : bascule vers des chemins redondants en quelques secondes. |
| **Complexité** | Simple à configurer pour les petits réseaux. | Complexe à déployer initialement, mais gestion simplifiée pour les grands réseaux. |
| **Convergence** | Aucune convergence nécessaire (routes fixes). | Convergence rapide grâce à l’algorithme SPF (Shortest Path First). |
| **Utilisation typique** | Réseaux petits/statiques avec peu de changements (ex : réseaux domestiques). | Réseaux complexes/dynamiques (ex : entreprises, datacenters) nécessitant redondance. |
| **Gestion de la redondance** | Requiert une configuration manuelle des routes de secours. | Gère automatiquement les chemins redondants (ex : liens multiples entre routeurs). |

### **Tableau 1:** Comparaison du routage statique et dynamique (OSPF) pour la haute disponibilité

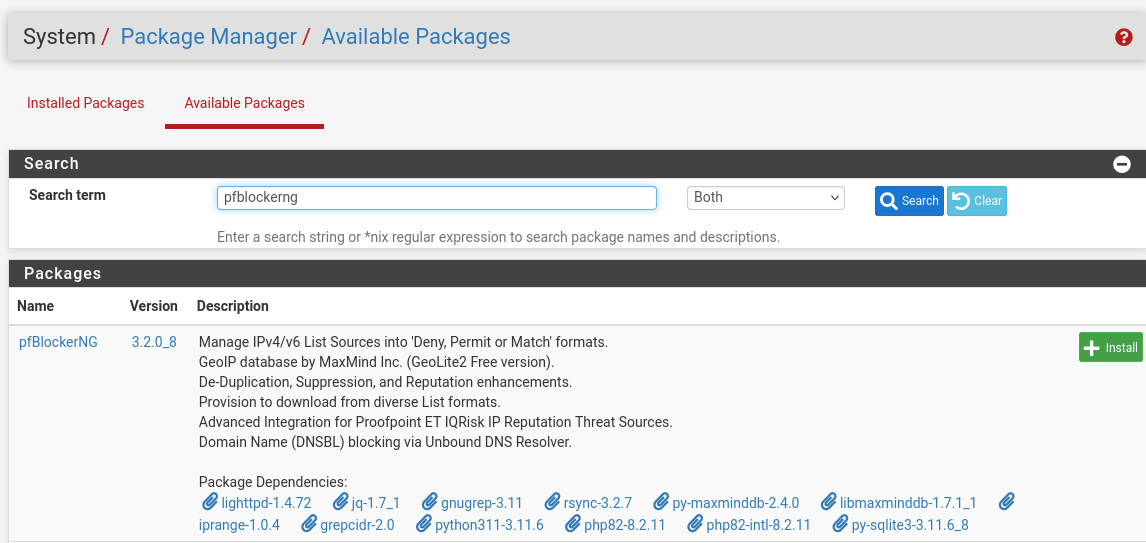
## **2.3 Présentation de pfSense : Fonctionnalités essentielles**

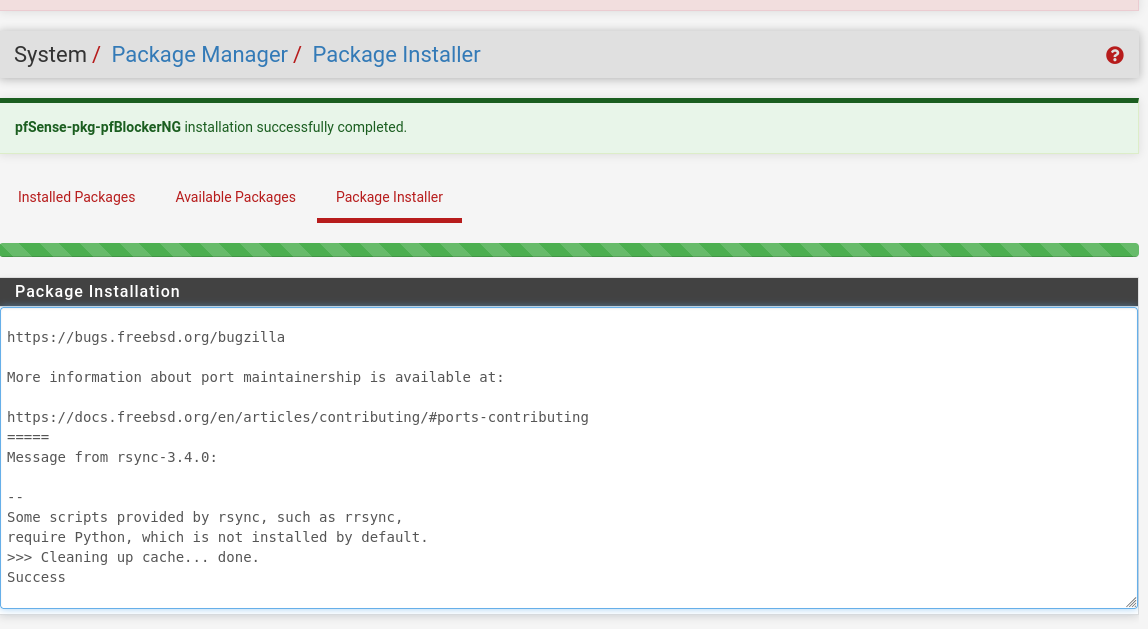
### **2.3.1 Modules avancés : pfBlockerNG, SquidGuard, Snort**

pfSense offre une gamme de modules avancés qui augmentent ses capacités de sécurité et de filtrage :

* **pfBlockerNG** : Module permettant de bloquer les adresses IP ou les domaines spécifiques via des listes noires. Il permet également de gérer des listes d'IP en fonction de sources externes et d'appliquer des restrictions géographiques pour limiter l'accès à certains pays ou régions.
* **SquidGuard** : Module de filtrage d’URL conçu pour restreindre l’accès à des sites web non autorisés ou potentiellement dangereux. Il peut être utilisé en complément du proxy Squid pour affiner les politiques d'accès et bloquer les contenus inappropriés.
* **Snort** : Système de Détection et de Prévention des Intrusions (IDS/IPS) permettant de surveiller en temps réel le trafic réseau, d’identifier des comportements suspects et de bloquer automatiquement les menaces avant qu'elles ne compromettent le réseau.

Ces modules offrent une couche de protection supplémentaire et permettent d’adapter pfSense aux besoins spécifiques de chaque infrastructure réseau. Leur combinaison permet une défense en profondeur en assurant à la fois le filtrage des contenus, la restriction des accès et la détection des activités malveillantes. Une bonne configuration et un suivi régulier de ces outils garantissent une meilleure sécurité et une gestion optimisée du trafic réseau.





**Figure 14:** Installation du pfBlockerNG

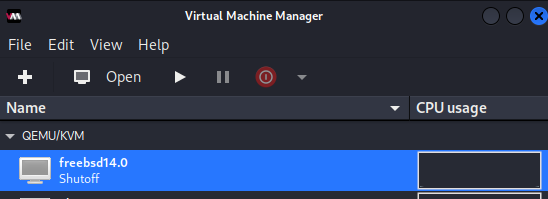
## 

## **2.4 Virtualisation : Environnement de test**

### **2.4.1 Déploiement de pfSense sous KVM et VMware**

Le déploiement de pfSense dans un environnement virtuel offre flexibilité et performance, permettant de tester différents scénarios sans compromettre l’infrastructure physique. Deux des hyperviseurs les plus populaires pour déployer pfSense sont KVM ou VMware.

* **KVM** : Ce système de virtualisation basé sur Linux permet de déployer pfSense dans un environnement virtuel pour tester des configurations de réseaux complexes.



**Figure 15:** Installation de pfSense sous KVM, Voir annexes pour plus de détails.

### 

### **2.4.2 Tests et problèmes rencontrés en lab**

Lors du déploiement de pfSense en environnement de test, plusieurs défis peuvent survenir :

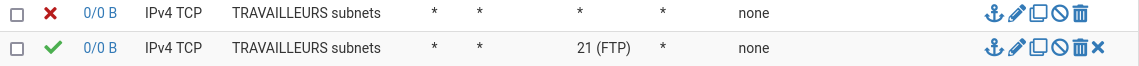
* **Problèmes de compatibilité réseau** : La configuration des VLANs et des interfaces réseau dans un environnement virtuel peut parfois être délicate, notamment avec KVM ou VMware, nécessitant des ajustements pour assurer la bonne communication.
* **Performance des ressources** : La machine hôte doit être dimensionnée correctement pour éviter des problèmes de latence ou de performance, surtout lorsque plusieurs machines virtuelles sont déployées simultanément.
* **Problèmes de connectivité** : Les erreurs de configuration des règles de pare-feu ou du routage peuvent bloquer la communication entre les VLANs ou perturber la connectivité du réseau virtuel.

### **Problème rencontré dans pfSense : Ordre Incorrect des Règles de Pare-feu**

Lors de la configuration des règles de pare-feu dans pfSense, un problème survient lorsque la règle de blocage généra**l** est placée avant la règle d'autorisation FTP.

Dans cet exemple, tout le trafic provenant du réseau Travailleurs est bloqué par une règle générale, y compris le trafic FTP (port 21). Cependant, une autre règle est configurée pour autoriser spécifiquement le trafic FTP.

Le problème réside dans l'ordre des règles : pfSense traite les règles de haut en bas, et si la règle de blocage est placée en premier, elle supprime tout le trafic avant que la règle d'autorisation FTP ne soit évaluée. En conséquence, le trafic FTP est silencieusement supprimé, et les utilisateurs du réseau Travailleurs ne peuvent pas accéder au service FTP.



**Figure 16 :** Ordre Incorrect des Règles

### **Solution : Inverser l'Ordre des Règles**

Pour résoudre ce problème, il est essentiel de réorganiser l'ordre des règles de pare-feu. La règle d'autorisation FTP doit être placée avant la règle de blocage général. Cela garantit que le trafic FTP est autorisé avant d'être évalué par la règle de blocage.



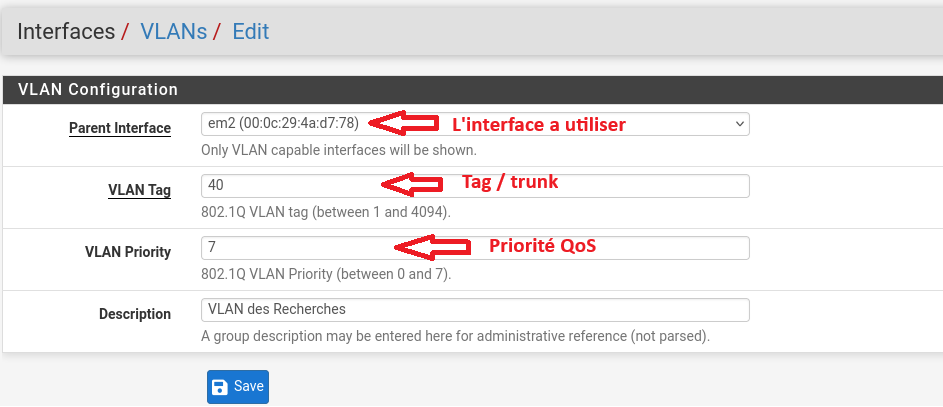
**Figure 17 :** Ordre Correct des Règles

# **Chapitre 3 : Mise en place des configurations de base**

## **3.1 Création du VLAN Recherche et segmentation réseau**

### **3.1.1 Définition du VLAN Recherche dans pfSense**

Le VLAN Recherche est créé pour répondre aux besoins spécifiques de l’équipe de recherche. Il permet d'isoler le trafic lié à cette équipe du reste du réseau, offrant ainsi une couche de sécurité supplémentaire. Cette isolation garantit que le trafic de recherche reste distinct des autres segments, tout en étant entièrement contrôlé et géré. L'objectif est d'assurer une gestion dédiée et sécurisée des communications au sein du réseau de recherche.



**Figure 18 :** Création du VLAN Recherche dans pfSense.



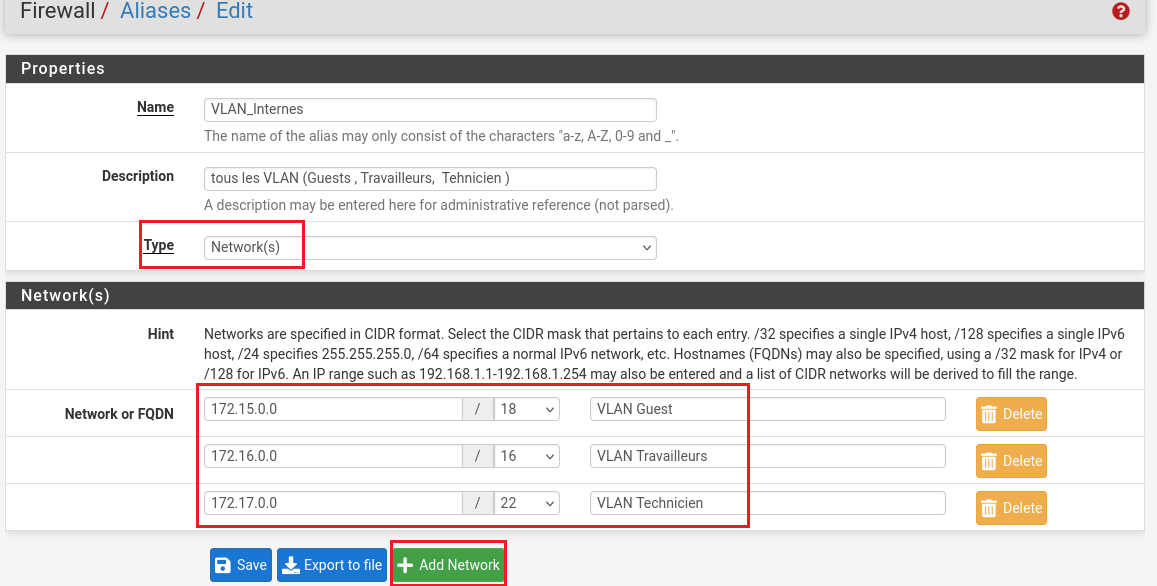
**Figure 19 :** Architecture générale du réseau cible (version finale)

## **3.1.2 Configuration du routage et du filtrage inter-segments pour le VLAN Recherche**

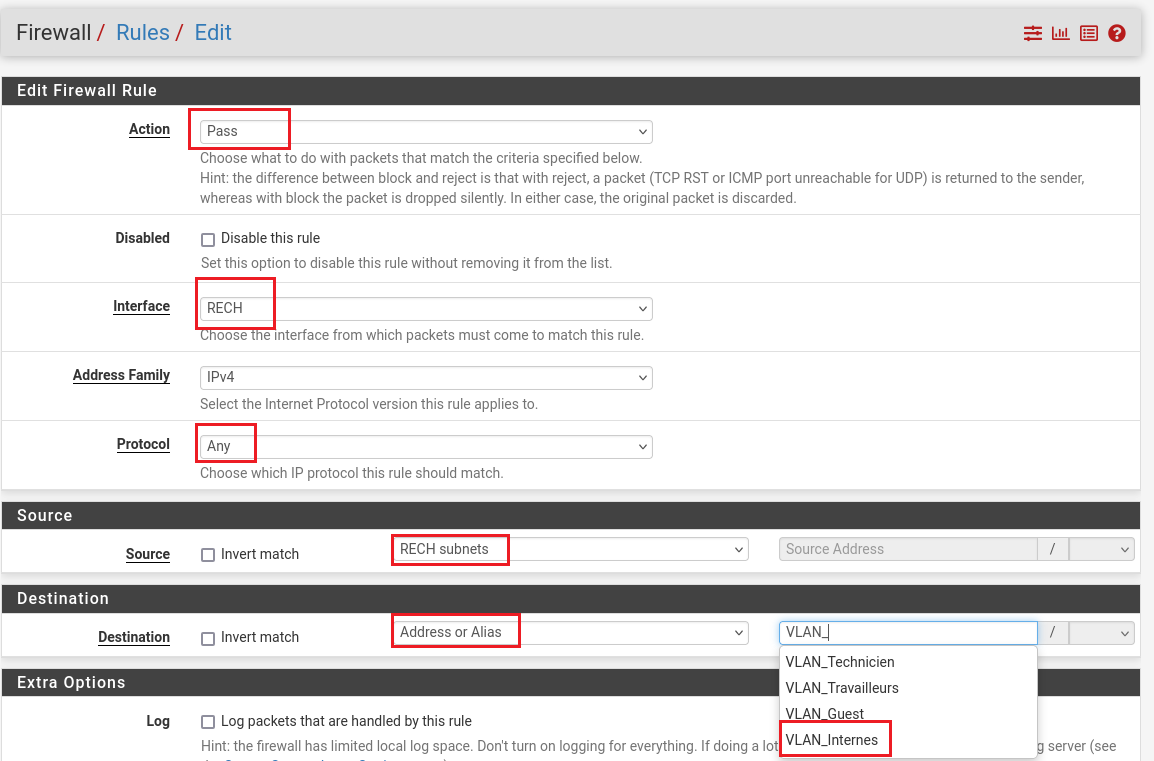
Le routage entre les VLANs est effectué au niveau du pare-feu pfSense. Au début, il est préférable de créer les règles de sorte que tous les VLANs puissent communiquer entre eux. Ensuite, les règles de filtrage ou de blocage inter-VLAN seront mises en place pour restreindre l'accès selon les besoins spécifiques.

Le VLAN Recherche est créé pour permettre un accès direct aux ressources nécessaires tout en assurant un contrôle strict sur la sécurité du trafic. Ce VLAN peut accéder à tous les alias et à Internet via le WAN, mais tout accès depuis le WAN ou d'autres interfaces vers le VLAN Recherche est bloqué. Cette restriction est mise en place pour protéger ce VLAN, considéré comme sensible, et garantir l'isolement du trafic de recherche des autres segments du réseau.

Les règles de filtrage sur pfSense doivent être configurées pour bloquer toute tentative d'accès extérieur tout en autorisant les communications internes et vers Internet selon les besoins.



**Figure 20:** Création d’un Allias pour grouper tous les VLAN internes.



**Figure 21:** Configuration d’une règle de pare-feu pour le VLAN Recherche pour permettre l'accès à tous les VLAN internes.



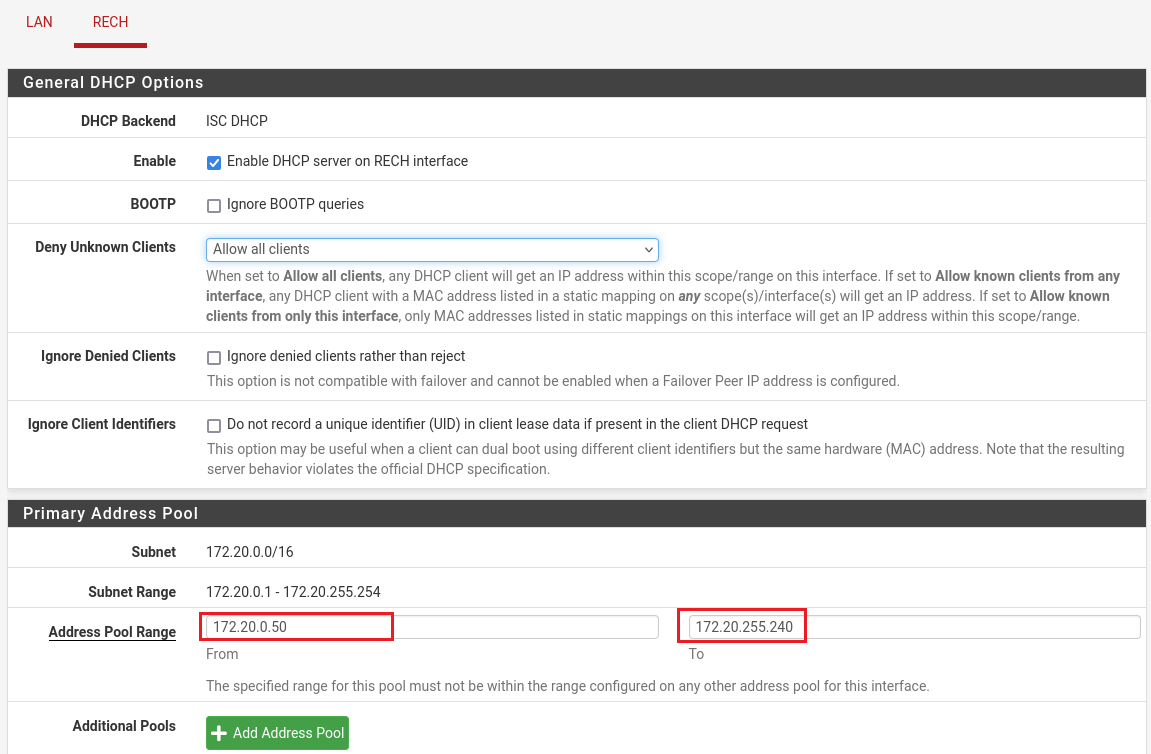
**

**Figure 21’:** Configuration d’une règle de pare-feu pour bloquer l'accès depuis tous les VLAN Internes vers VLAN Recherche + résultat.

## **3.2 Configuration DHCP/DNS pour le VLAN Recherche**

### **3.2.1 Assignation d’adresses IP et serveurs DNS**

Le serveur DHCP de pfSense est activé sur le VLAN Recherche. Une plage d’adresses (par exemple, 172.20.0.1 à 172.20.255.254) est définie. Les serveurs DNS de recherche sont également attribués pour gérer les résolutions locales. Cette configuration permet de centraliser l’attribution des adresses et du DNS.

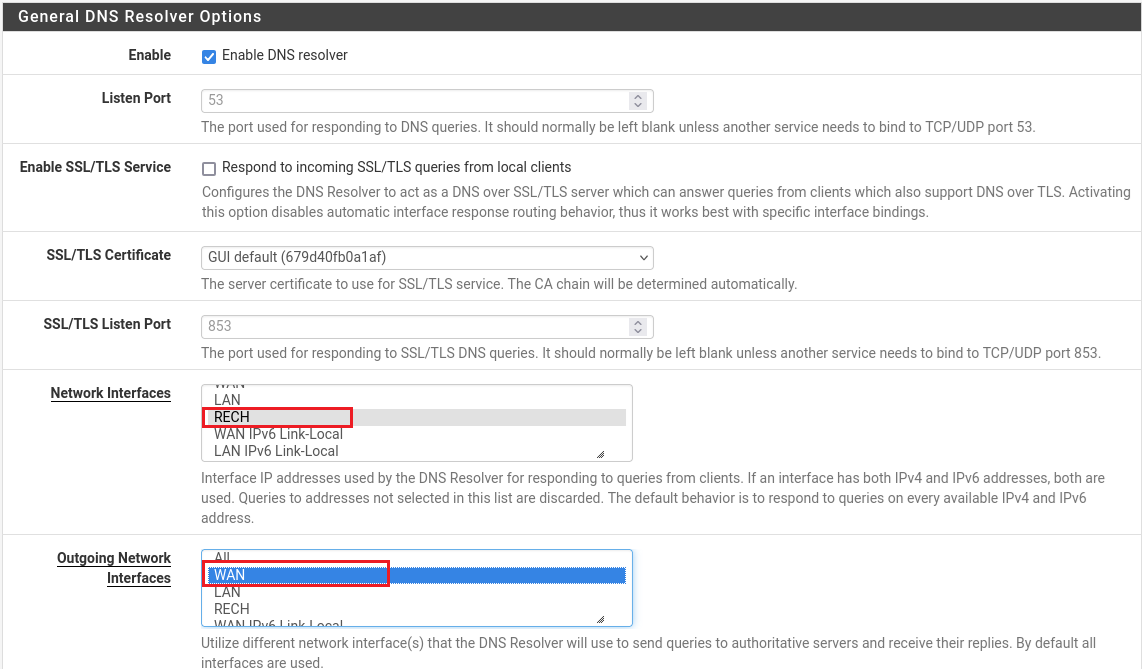


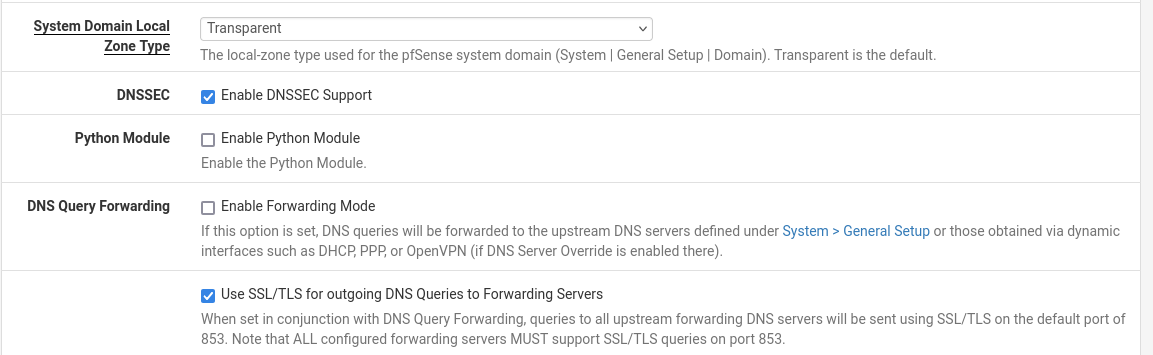
**Figure 22:** Configuration DHCP pour le VLAN Recherche. (Services>DHCP>ServerRECH)

### 

### **3.2.2 Choix et configuration entre DNS Forwarder et DNS Resolver**

* Le DNS Forwarder (dnsmasq) est un service qui redirige les requêtes DNS vers des serveurs externes, sans effectuer de résolution directe. Il est rapide et léger mais dépend des serveurs en amont, ce qui peut poser des risques de sécurité.
* Le DNS Resolver est configuré pour une résolution récursive locale, assurant une sécurité renforcée. Il prend en charge DNSSEC (sécurisation des réponses DNS contre les falsifications) et SSL/TLS (chiffrement des requêtes DNS pour éviter l’interception). Ces technologies garantissent une résolution DNS fiable et protégée contre les attaques. Toutes les requêtes envoyées aux serveurs de redirection utilisent SSL/TLS sur le port 853, nécessitant une prise en charge de ce protocole par les serveurs en amont.





**Figure 23:**  Captures d’écran des configurations du DNS Resolver avec activation de DNSSEC et SSL/TLS dans pfSense.

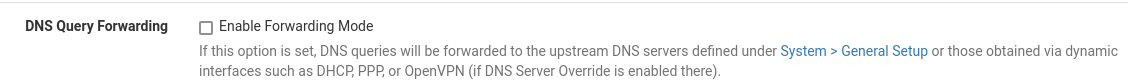
| **Critère** | **DNS Resolver (Unbound)** | **DNS Forwarder (dnsmasq)** |
| --- | --- | --- |
| **Méthode de**  **résolution** | Résolution récursive locale | Redirige les requêtes vers des serveurs externes |
| **Sécurité** | Sécurisé avec DNSSEC et SSL/TLS | Dépend des serveurs en amont, moins sécurisé |
| **Dépendance externe** | Aucune, fonctionne de manière autonome | Dépend des serveurs DNS configurés |
| **Performance** | Peut être plus lent au premier accès mais efficace avec le cache | Plus rapide initialement mais moins sécurisé |
| **Utilisation des ressources** | Plus gourmand en CPU/RAM | Léger et rapide |
| **Utilisation recommandée** | Réseaux sécurisés et autonomes (ex. VLAN Recherche) | Environnements nécessitant un accès rapide aux DNS externes |

### **Tableau 2 :** Comparaison entre DNS Resolver et DNS Forwarder

#### 

### **3.2.3 Gestion des résolutions DNS et blocage des DNS externes**

Unbound est configuré pour ne pas transmettre les requêtes DNS à l’extérieur. Cela bloque l'accès à des serveurs DNS non autorisés. Les résolutions DNS sont ainsi sécurisées et gérées en interne. Cette configuration prévient les risques de fuite de données.

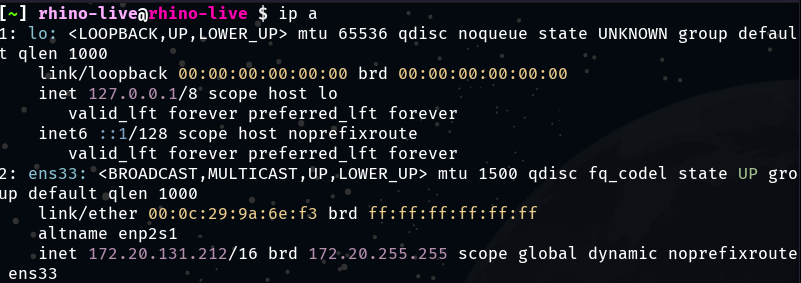


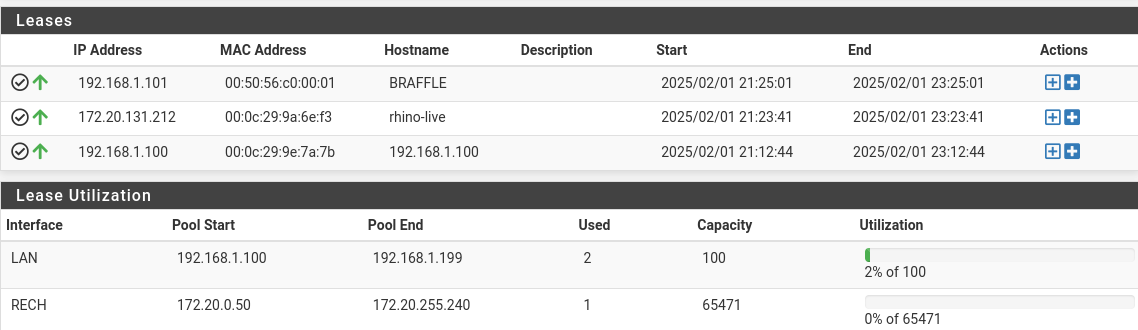
**Figure 24:** Capture d’écran de la configuration du DNS Resolver (Unbound) dans pfSense.

## **3.3 Vérifications et tests de connectivité**

### **3.3.1 Validation de l’attribution des adresses DHCP**

Supposons que nous disposions d'un switch qui supporte le VLAN tagging. Les baux DHCP sont vérifiés sous Status > DHCP Leases. Cette étape assure que les appareils du VLAN Recherche reçoivent les bonnes adresses IP. Elle permet aussi de valider le bon fonctionnement du service. Toute anomalie dans l’attribution est rapidement détectée.

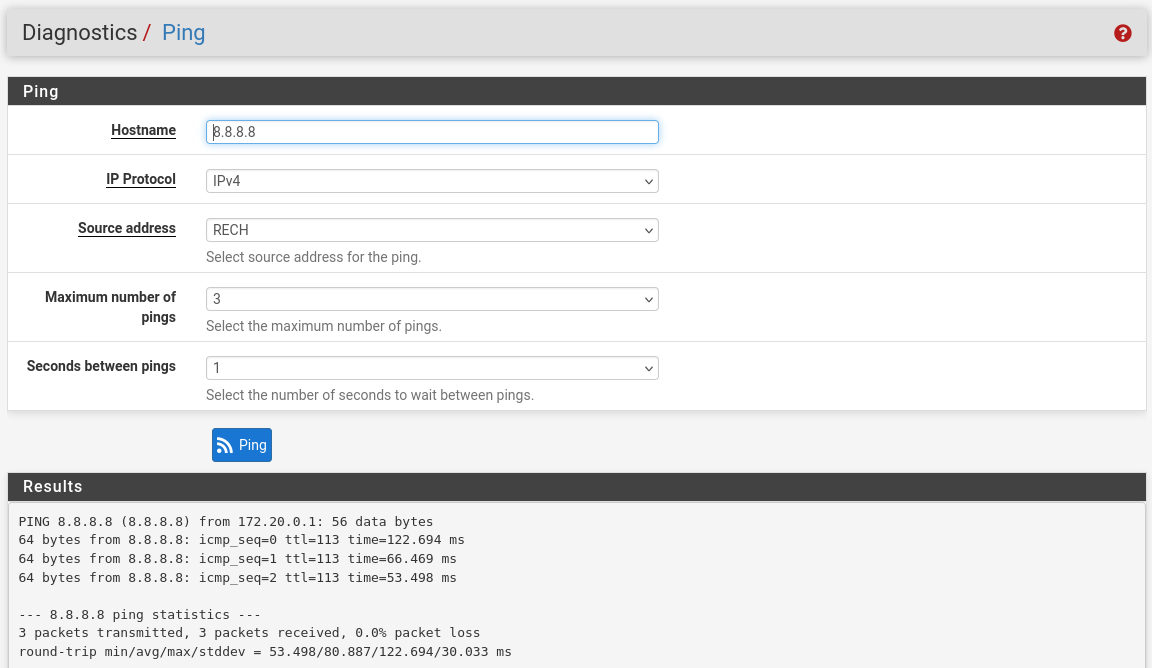




**Figure 25:** Capture d’écran des baux DHCP attribués dans pfSense et dans la machine qui est dans le VLAN Recherche.

### **3.3.2 Utilisation de l'outil de diagnostic**

L'outil Diagnostics de pfSense offre de nombreuses fonctionnalités pour diagnostiquer et surveiller votre réseau. Par exemple, nous allons essayer la fonction Ping. Cette option permet d'envoyer des requêtes ICMP vers une adresse cible (comme 8.8.8.8, le serveur DNS de Google) pour vérifier la connectivité, mesurer la latence et détecter d’éventuelles pertes de paquets. Ces informations sont essentielles pour identifier et résoudre rapidement des problèmes de réseau.



**Figure 26 :** Capture d’écran du test Ping depuis le VLAN recherche vers 8.8.8.8

### **3.3.3 Analyse des logs système**

Les Syslogs de pfSense (via Status > System Logs > System) offrent une vue détaillée des activités du système. Leur analyse permet de :

* Suivre l'état des services : surveiller démarrages, arrêts et redémarrages (ex. DHCP, DNS, VPN).
* Détecter erreurs et alertes : repérer rapidement les messages d’erreur ou d’authentification et les avertissements matériels.
* Vérifier les règles de pare-feu : s'assurer que les règles autorisant ou bloquant le trafic se déclenchent comme prévu.
* Filtrer les événements : cibler par date, IP, port ou type d’erreur pour une analyse efficace en cas d'incident.

#### 

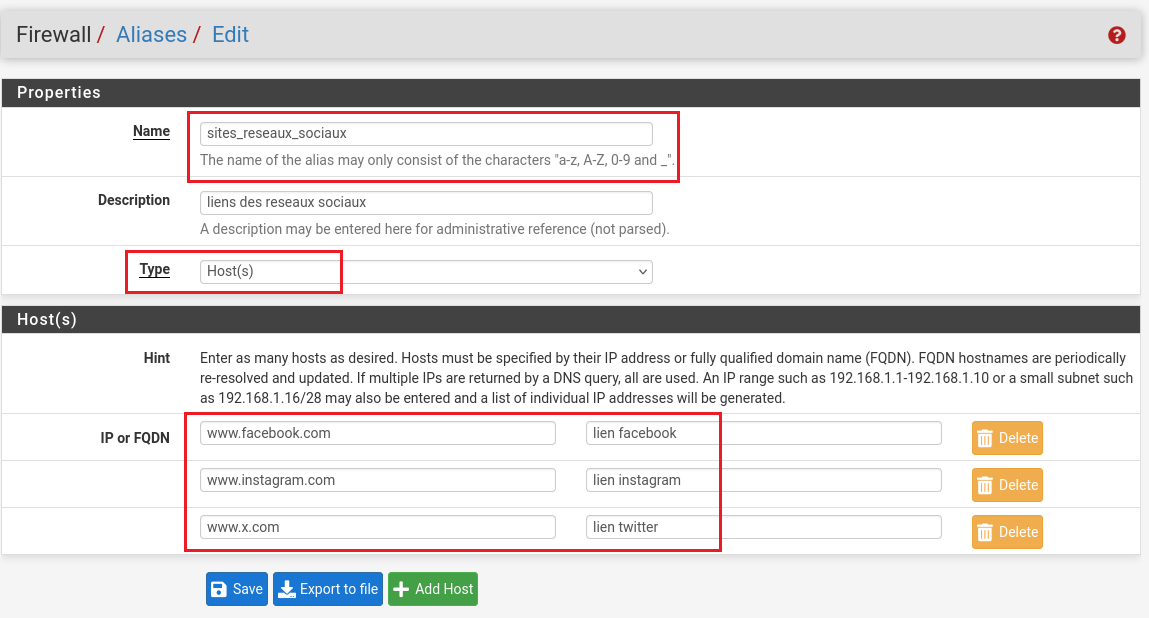
**Figure 27 :** Capture d’écran des logs système dans pfSense (SysLogs Général)

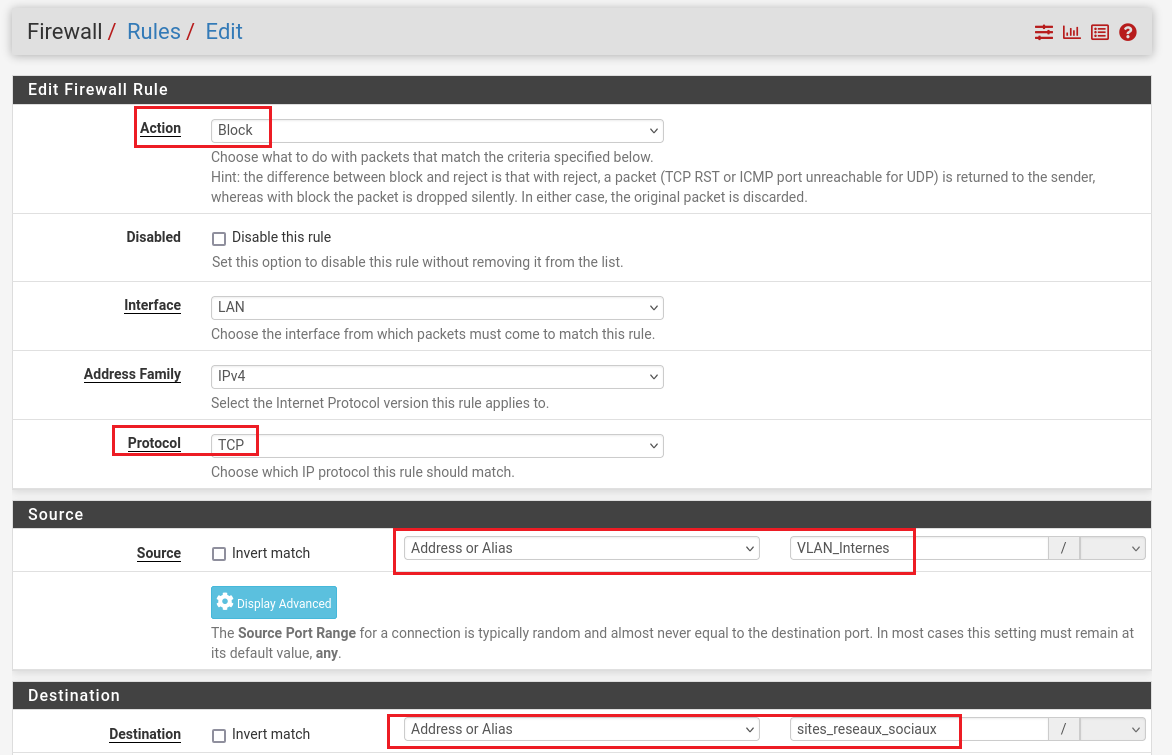
# **Chapitre 4 : Mise en œuvre du filtrage avec pfSense**

## **4.1 Filtrage des sites web et restrictions d’accès**

### **4.1.1 Blocage par règles et alias**

Dans cette méthode, des alias contenant des adresses ou noms de domaine indésirables sont créés. Des règles de pare-feu sont ensuite configurées pour bloquer l'accès aux sites listés dans ces alias.  
 Ce blocage permet d'empêcher les utilisateurs d'accéder aux sites inappropriés ou non sécurisés.  
 Les règles sont appliquées directement sur les interfaces du VLAN concerné via pfSense.

  
 **Figure 28 :** Création d'aliases des sites à bloquer



**Figure 29 :**Configuration du blocage par règles et alias dans pfSense .

### **4.1.2 Filtrage par Domain Override en DNS**

Cette technique consiste à rediriger les requêtes DNS pour certains domaines vers une destination personnalisée .  
 Le Domain Override permet de contrôler la résolution des noms de domaine critiques, forçant une réponse personnalisée.

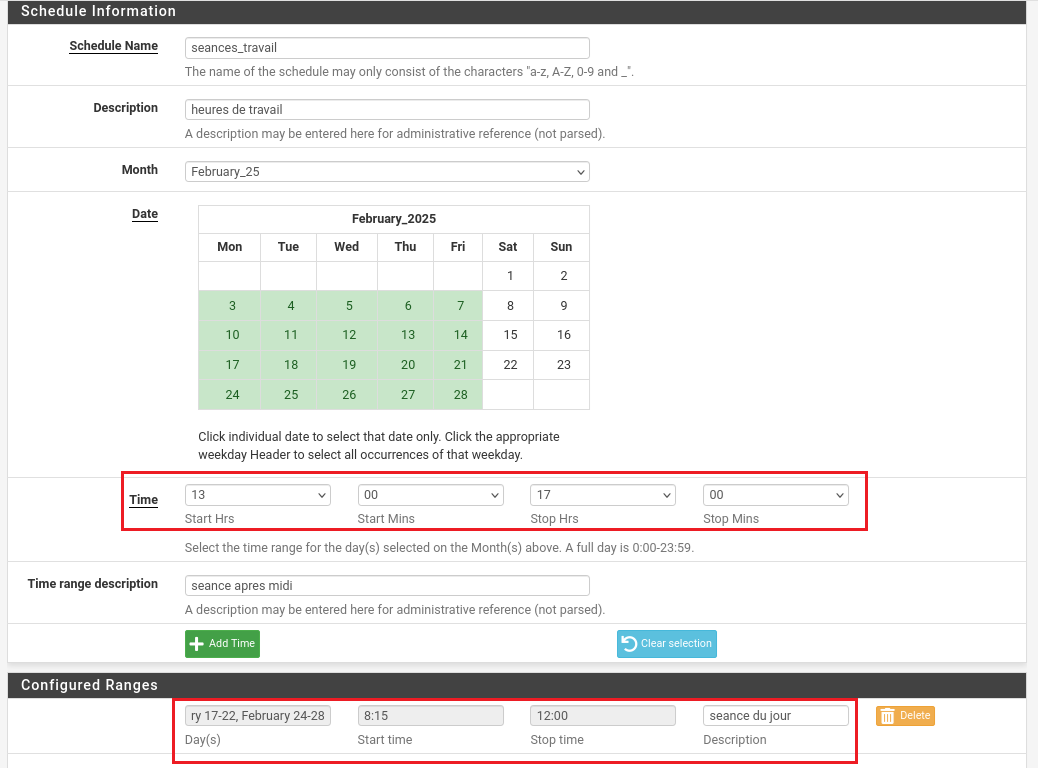
  
 **Figure 30 :** Configuration du Domain Override dans l’interface DNS vers une adresse non routable.

#### 

## **4.2 Gestion des accès selon un planning et pfBlockerNG**

### **4.2.1 Planification des blocages selon les horaire**

La gestion des accès par planning contrôle l’accès à Internet ou à certains services selon des horaires définis. Avec pfSense et pfBlockerNG, on peut restreindre des sites ou applications à des périodes précises. pfSense gère les règles de pare-feu programmées, tandis que pfBlockerNG bloque des catégories de sites. Leur combinaison permet un blocage dynamique, optimisant productivité et sécurité.

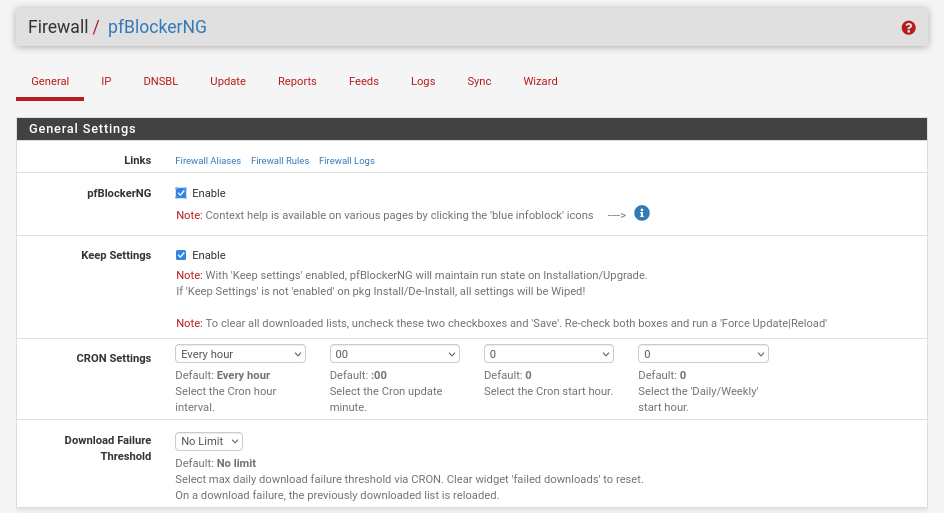


**Figure 31 :** Interface de configuration des schedules dans pfBlockerNG illustrant la planification des blocages (Firewall > Schedules > Edit) .

### **4.2.2 Filtrage avancé avec pfBlockerNG et planification (schedules)**

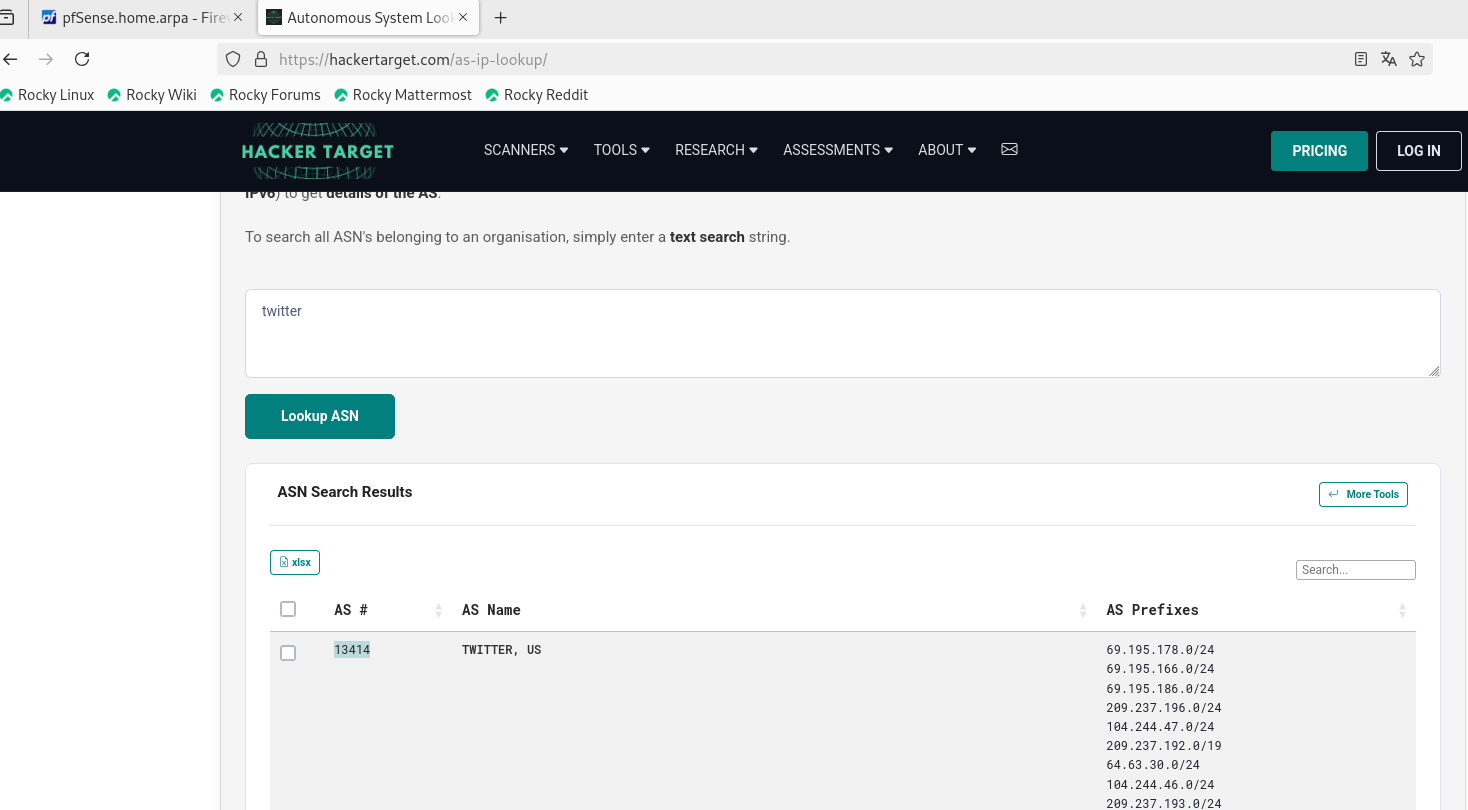
Nous configurons actuellement pfBlockerNG, un puissant outil de filtrage de contenu dans pfSense, afin de bloquer des sites web spécifiques ou des catégories de sites. Cette configuration sera appliquée aux VLAN Technicien et VLAN Travailleurs à l'aide d'une règle de pare-feu intégrant un planning basé sur le temps.

En combinant les capacités de blocage de sites web de pfBlockerNG avec une règle de planification, nous pouvons restreindre dynamiquement l'accès à certains sites pendant des périodes définies, comme les heures de travail.



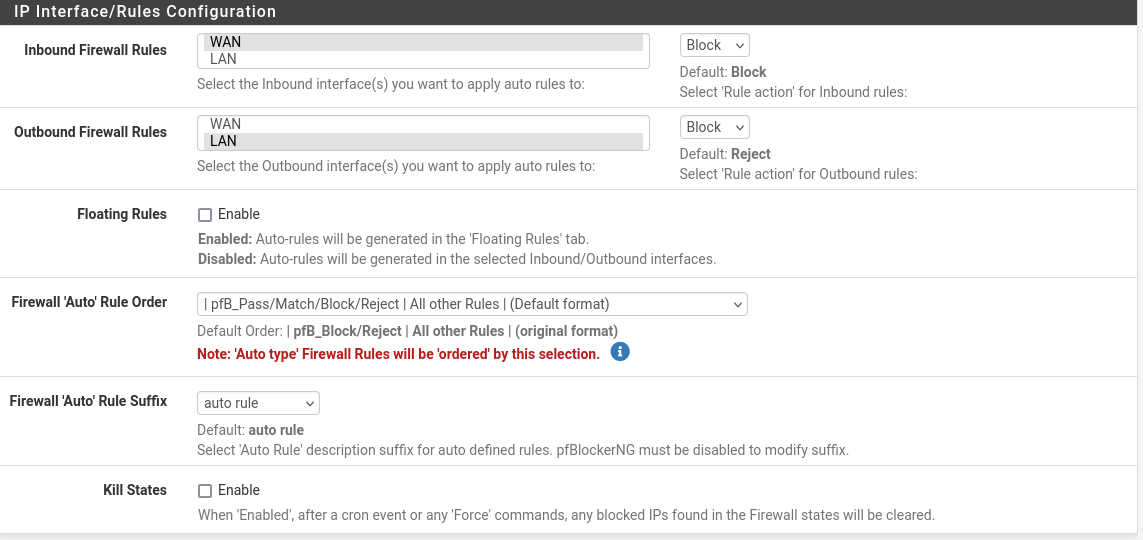
**Figure 32 :** Interface generale de pfBlockerNG (Firewall > pfBlcokerNG).

* Afin d'affiner le filtrage, nous allons utiliser les numéros de système autonome (ASN) pour bloquer certaines plages d'adresses IP associées à des services spécifiques.

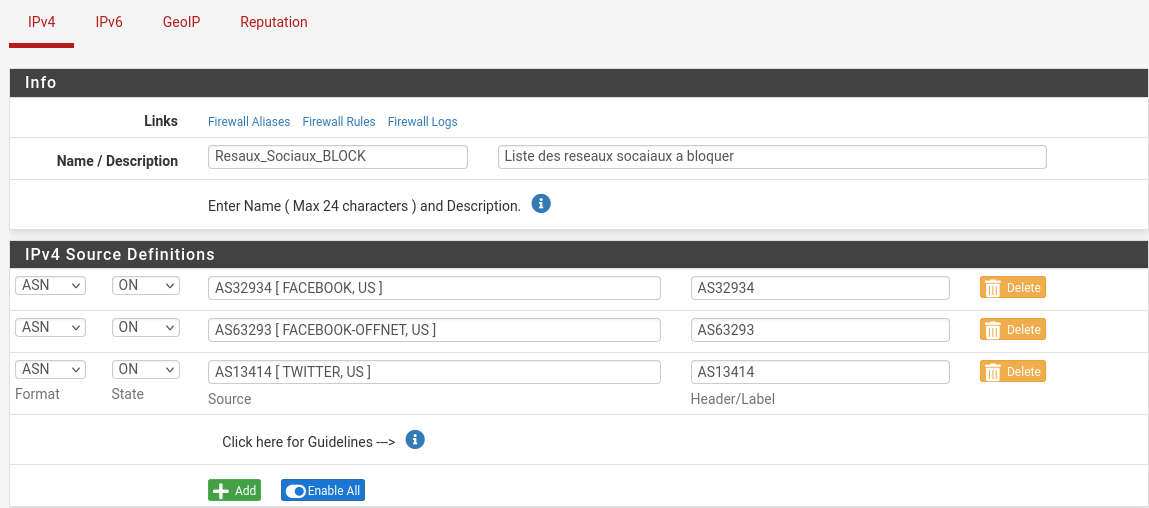


**Figure 32 :** Le site web utilisé pour récupérer ces ASN (hackertarget).

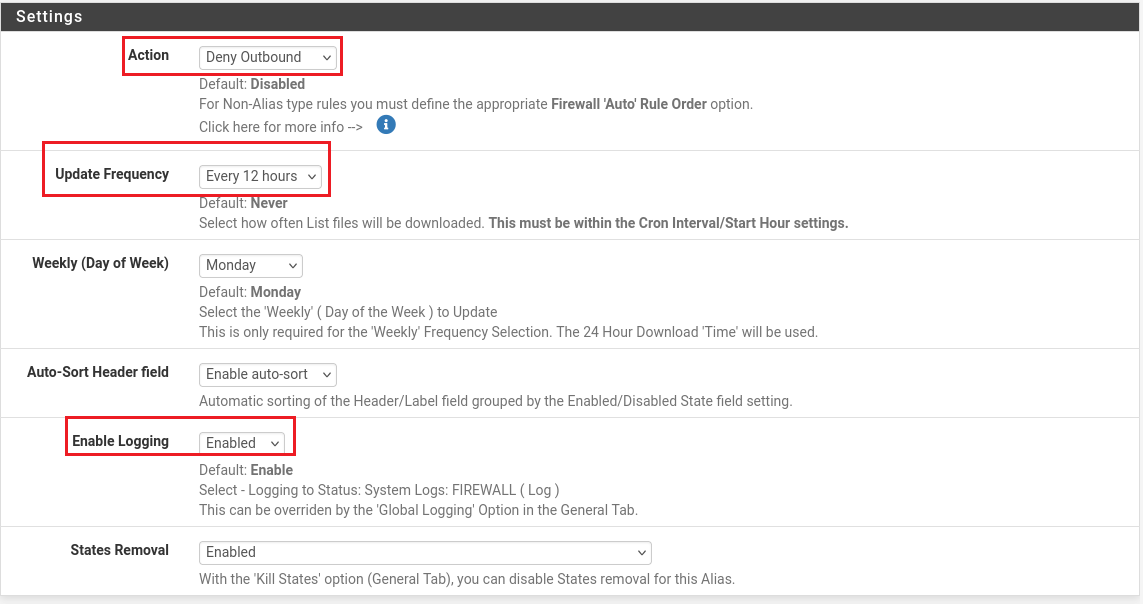
* Dans pfBlockerNG, la configuration des règles de pare-feu suit une logique inversée par rapport aux règles classiques de pfSense. Ici, les règles Inbound et Outbound sont toutes deux définies sur Block, empêchant à la fois les connexions entrantes depuis les IPs listées et le trafic sortant vers des destinations bloquées. Cela renforce le filtrage en bloquant activement toute communication indésirable dans les deux directions.



**Figure 33 :** Configuration des règles Inbound et Outbound dans pfBlockerNG sous (Firewall > pfBlockerNG > IP)



**Figure 34 :** Attribution des ASN sous le pare-feu pfBlockerNG (IP > IPv4)



**Figure 35 :** Configuration des paramètres

* Cette Figure montre la configuration des paramètres de la regle du filtrage :
* Action : Deny Outbound → Le filtrage s'applique au trafic sortant, bloquant les connexions vers les IPs indésirables. L'option Deny Outbound sera appliquée sur le LAN pour empêcher les connexions non autorisées.
* Update Frequency : Every 12 hours → La liste des IPs bloquées sera mise à jour automatiquement toutes les 12 heures pour garantir une protection efficace.
* Enable Logging : Enabled → L'enregistrement des événements est activé, permettant de suivre les connexions bloquées dans les logs du pare-feu.
* Pour appliquer les modifications et télécharger les listes mises à jour, il est nécessaire de se rendre dans l'onglet Update de pfBlockerNG et de cliquer sur Run. Cette action permet de récupérer et d’installer les listes définies, assurant ainsi un filtrage efficace selon les règles configurées.

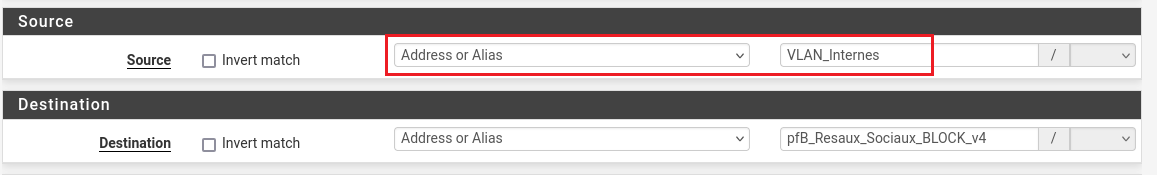


**Figure 36:** Exécution de la mise à jour des listes dans pfBlockerNG

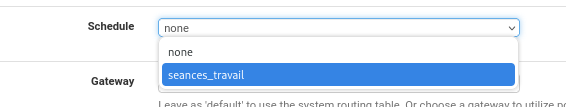
* Une nouvelle règle sera maintenant ajoutée sur l’interface LAN. Nous allons spécifier l’alias VLAN\_Internes comme source et appliquer un schedule pour contrôler les périodes d’accès. Cette règle permettra de restreindre l’accès selon les plages horaires définies tout en appliquant les filtres pfBlockerNG.



**Figure 37:** Règle de pare-feu avant configuration



**Figure 38**: Configuration de la règle avec l’alias VLAN\_Internes



**Figure 39 :** Configuration du planning (Schedule)

****

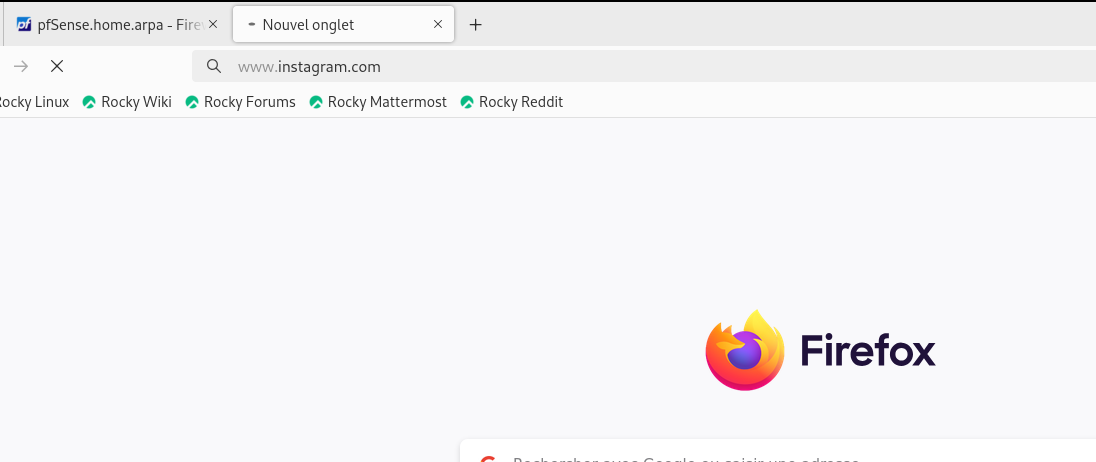
**Figure 40 :** Règle de pare-feu après configuration

# **Chapitre 5 : Application en environnement réel**

## **5.1. Filtrage par règles et alias**

### **5.1.1. Résultats et efficacité du blocage par règles et alias**

* Les résultats montrent que, bien que cette méthode ait fonctionné correctement pour certains sites, le blocage de Facebook a rencontré des difficultés techniques. Une fois que l'utilisateur est connecté, le blocage est contourné, ce qui réduit l'efficacité de la méthode dans certains cas.

  
 **Figure 41 :** blocage avec succès pour instagram.



**Figure 42 :** blocage échoue pour facebook.

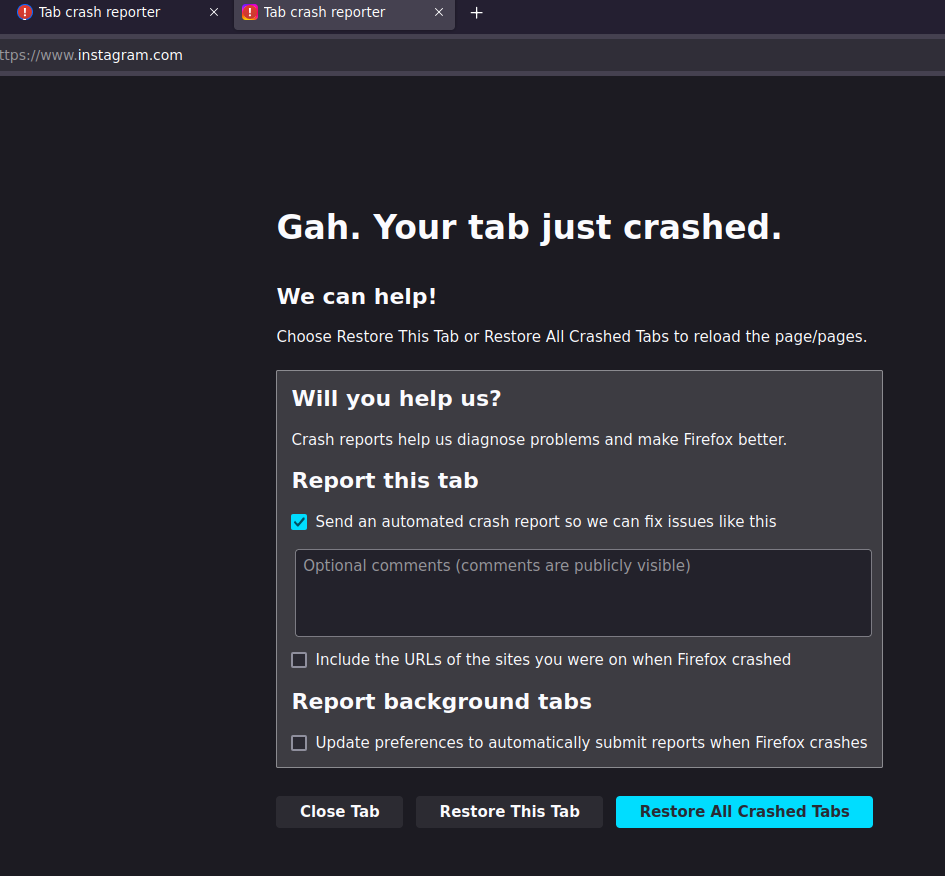
### **5.1.2. Problèmes rencontrés et solutions pour éviter les échecs**

* L'un des problèmes majeurs rencontrés était la lenteur du blocage sur Facebook, suivie d'une perte d'efficacité une fois la connexion établie. Aucune solution ne semblait efficace à part le changement de méthode. Les ajustements des règles ou l'utilisation de méthodes complémentaires n'ont pas permis de résoudre le problème de manière satisfaisante.

## **5.2. Filtrage par Domain Override en DNS**

### **5.2.1. Évaluation du fonctionnement de la redirection DNS**

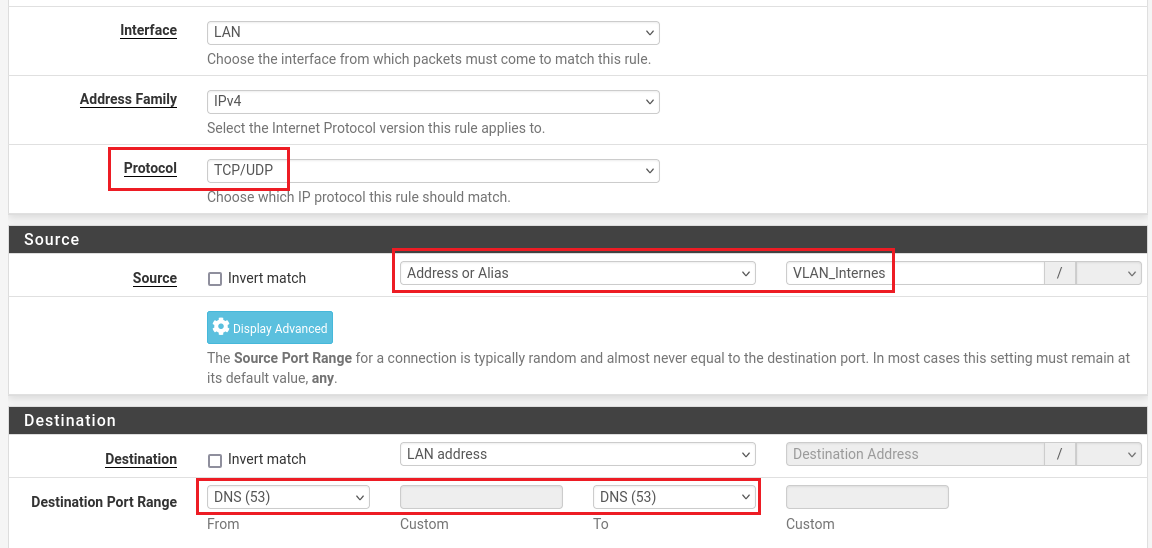
* Lorsque le filtrage DNS est appliqué, il empêche l'accès aux sites indésirables en redirigeant les requêtes DNS vers des serveurs contrôlés. Cependant, si l'utilisateur modifie manuellement son serveur DNS, le filtrage ne sera plus efficace, comme observé dans certaines situations.



**Figure 43 :** blocage avec succès pour facebook.

### **5.2.2. Difficultés constatées et stratégies pour les contourner**

* Le principal défi rencontré était la possibilité pour les utilisateurs de contourner la redirection DNS en modifiant leurs paramètres DNS. Une solution pour contrer ce problème serait de bloquer l'accès à des configurations DNS non autorisées via des règles de pare-feu.



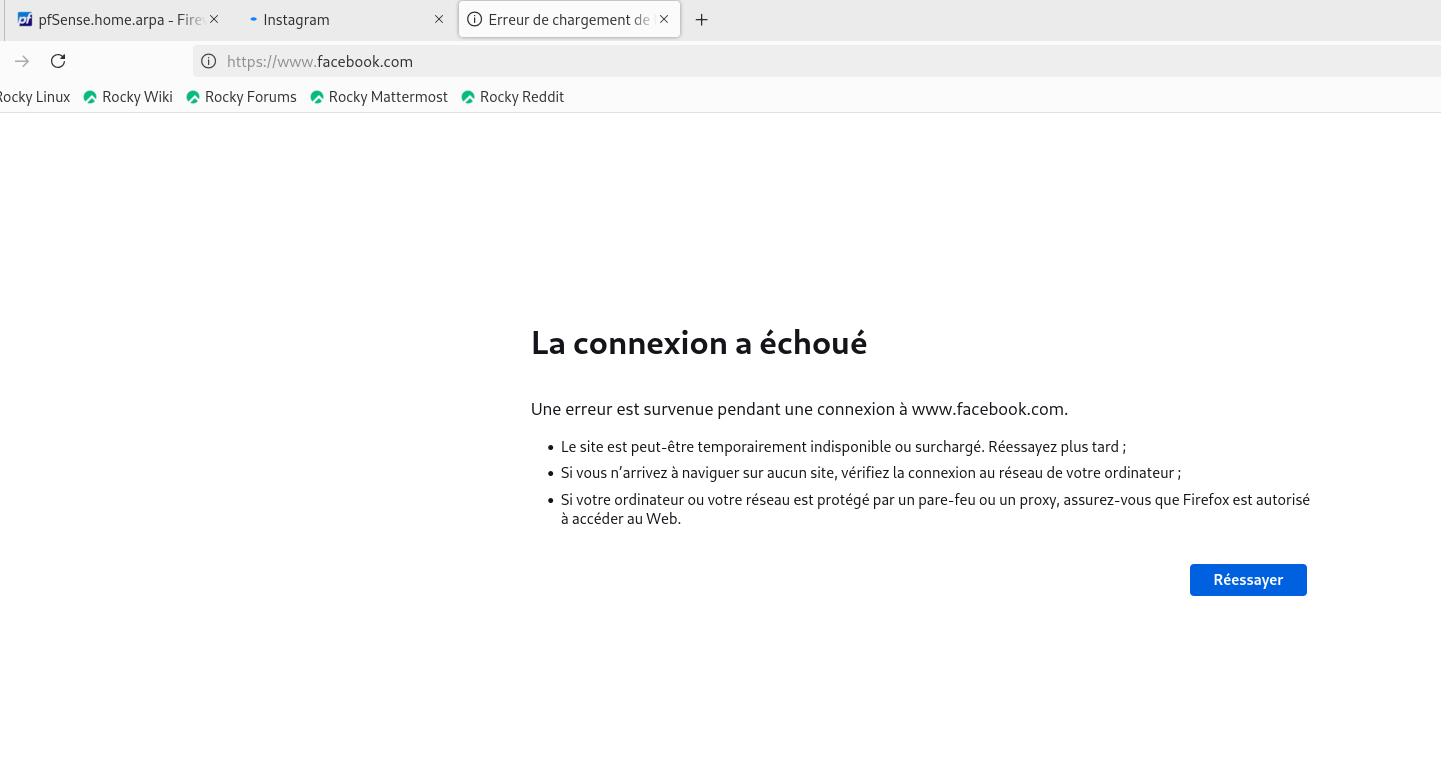
**Figure 44 :** Creation d’une regle sur le pare-feu pour bloquer le traffic vers un serveur DNS externe .

### 

## **5.3. Filtrage avancé avec pfBlockerNG et planification (schedules)**

### **5.3.1. Analyse des résultats de pfBlockerNG appliqué aux VLANs**

* L'application de pfBlockerNG aux VLANs a permis un filtrage avancé avec un minimum de problèmes. Les résultats ont montré une efficacité élevée dans le contrôle des accès à des sites indésirables, ce qui en fait la méthode de filtrage la plus performante parmi celles évaluées.



**Figure 45 :** blocage avec succès pour facebook.

# Conclusion générale

Ce stage chez New Technology Services Info m’a permis d’approfondir mes compétences en administration et sécurisation des réseaux à travers la configuration avancée de pfSense. L’objectif était de sécuriser une infrastructure VLAN (Administrateurs, Techniciens, Travailleurs) et d’implémenter des mécanismes de filtrage avancés.

J’ai acquis une expertise dans la segmentation réseau, le routage inter-VLAN, le NAT/PAT et l’utilisation de pfBlockerNG pour le blocage dynamique des sites non professionnels selon des plages horaires. La virtualisation sous KVM a facilité les tests et optimisations, malgré quelques défis techniques (priorisation des règles, performances du pare-feu ).

### **Résultats et Limites**

* Isolation renforcée des VLANs et meilleure gestion du trafic.
* Contrôle des accès via des règles strictes et DNS sécurisé (DNSSEC/SSL-TLS).
* Blocage dynamique des sites non professionnels avec pfBlockerNG.
* Contournement possible du filtrage DNS et difficulté à bloquer certaines plateformes (ex. Facebook).

Ce stage a consolidé mes compétences en réseaux et résolution de problèmes tout en mettant en avant l’importance de l’open source et de la virtualisation. Pour aller plus loin.

Cette expérience renforce mon engagement dans le réseaux des systèmes informatiques, un domaine exigeant où l’adaptation et l’innovation sont essentielles.

# Annexes

**KVM et virt-manager setup**

**CMD:**sudo apt install qemu-kvm libvirt-clients libvirt-daemon-system bridge-utils

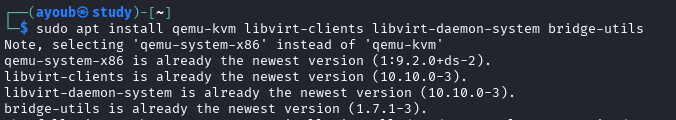
Cette commande installe les paquets nécessaires pour configurer et utiliser KVM (Kernel-based Virtual Machine) et QEMU pour la virtualisation sur Linux :

1. qemu-kvm : Le logiciel de virtualisation QEMU avec support KVM.

2. libvirt-client : Outils en ligne de commande pour gérer les machines virtuelles via libvirt.

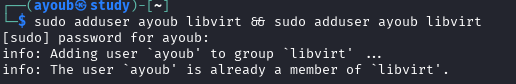
3. libvirt-daemon-system: Le service libvirt pour gérer les machines virtuelles.

4. bridge-utils: Utilitaires pour configurer des bridges réseau, utiles pour connecter les machines virtuelles au réseau.



**CMD:** sudo adduser ayoub libvirt && sudo adduser ayoub libvirt

Ces commandes ajoutent l'utilisateur ayoub aux groupes libvirt et kvm, ce qui lui permet de gérer des machines virtuelles sans avoir besoin de droits administrateur (sudo).



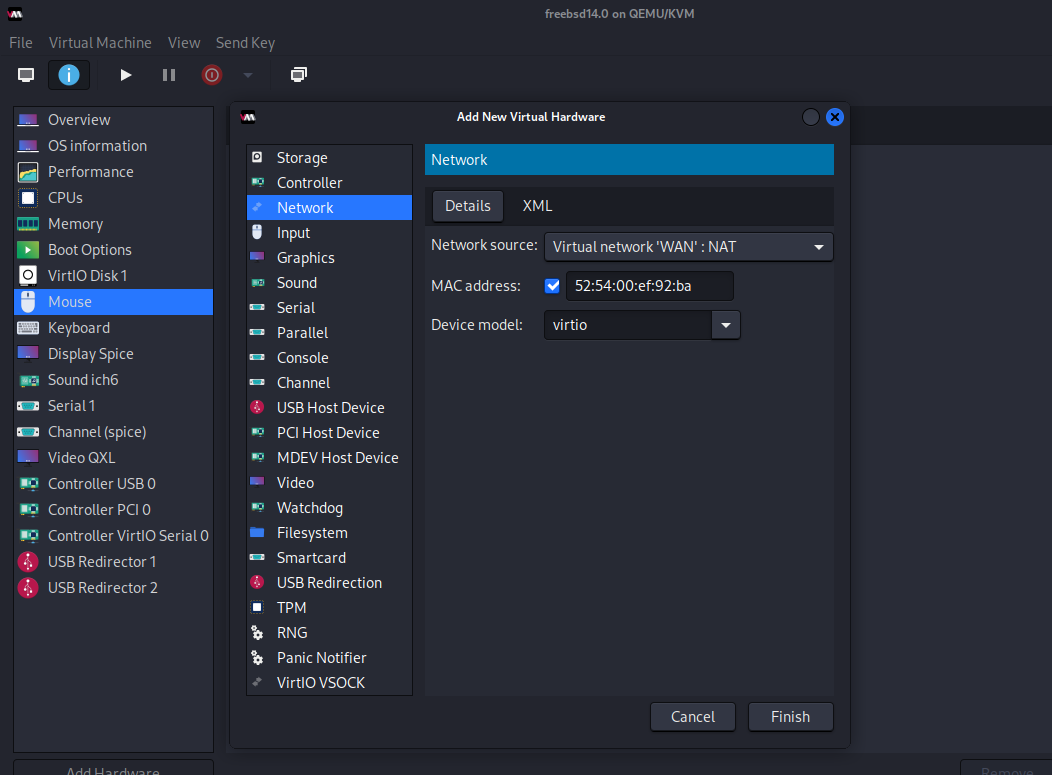
**CMD:** sudo apt install virt-manager

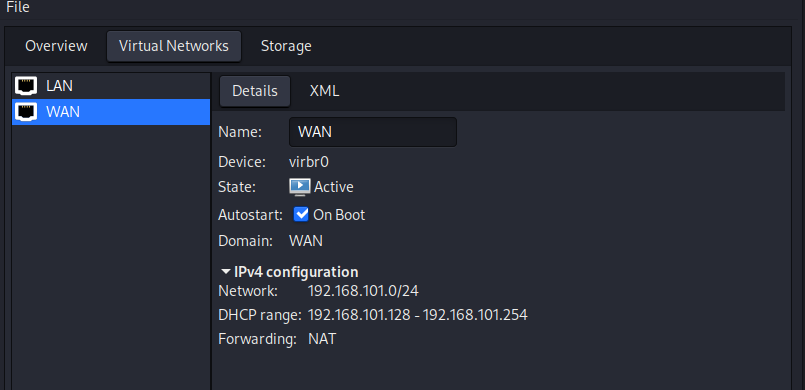
Cette commande permet d'installer virt-manager, un outil graphique pour gérer des machines virtuelles avec KVM/QEMU.



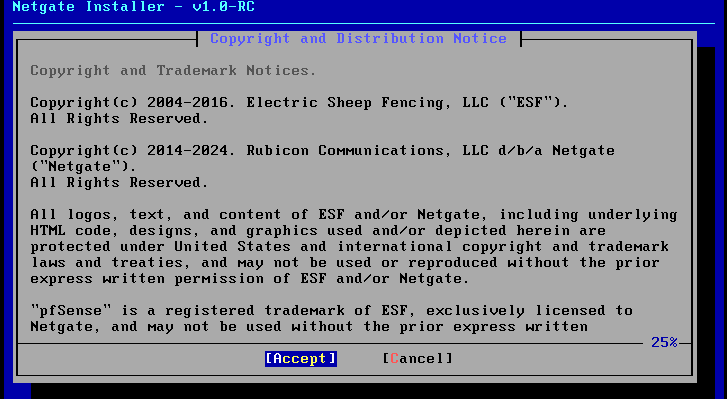
**pfsense Setup**

L’application des cartes réseaux virtuelles :

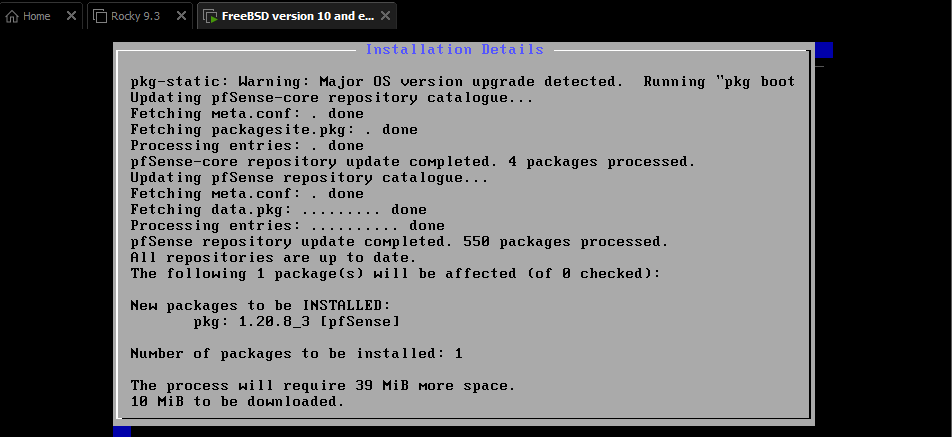




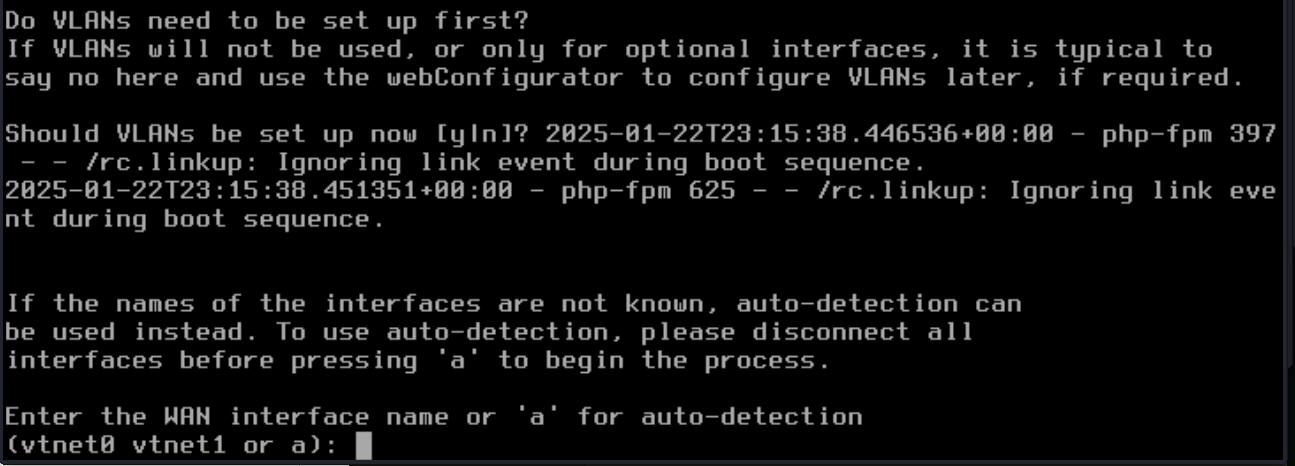
PUIS en mettre en marche la machine pfsense et en installe l’installation est très simple



Après cette étape :



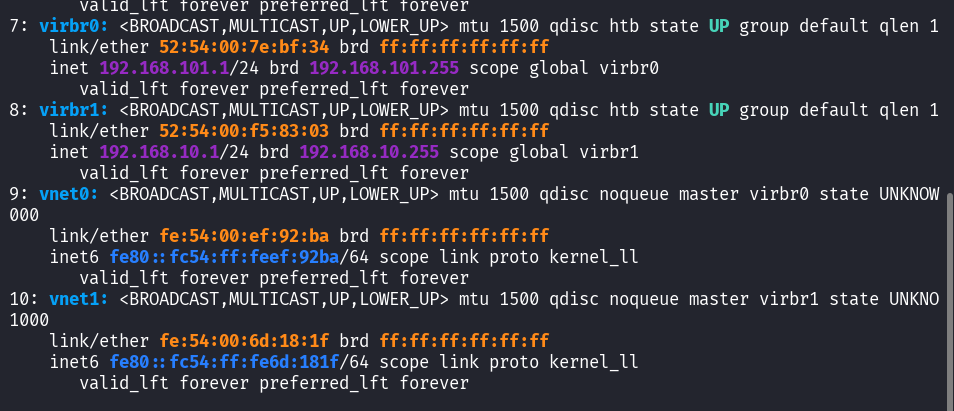
On est face à ce console :



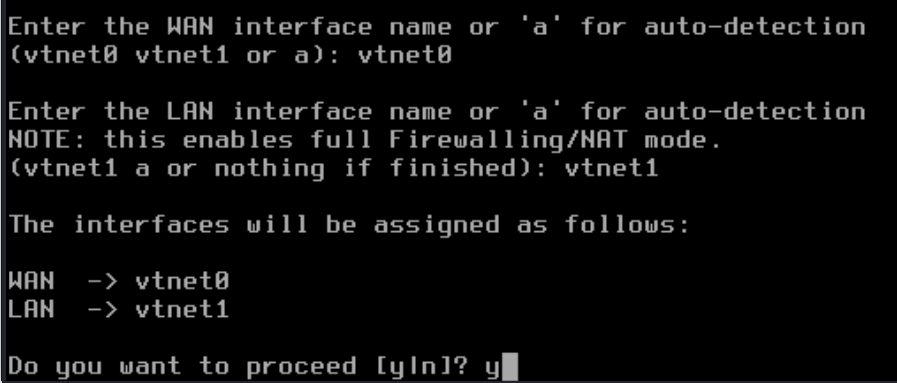
Il est toujours mieux de double check les cartes Utilisant :

* Ip a

Nous pouvons voir les plages d'adresses qui correspond à chaque carte



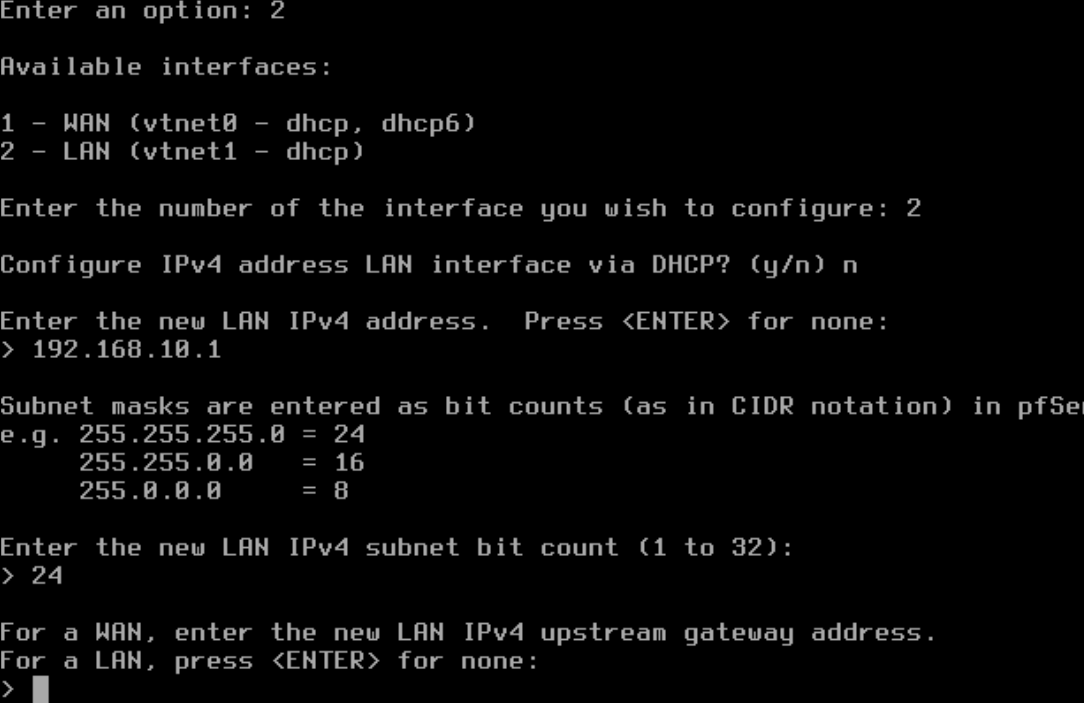
Puis on va compléter la configuration via console:

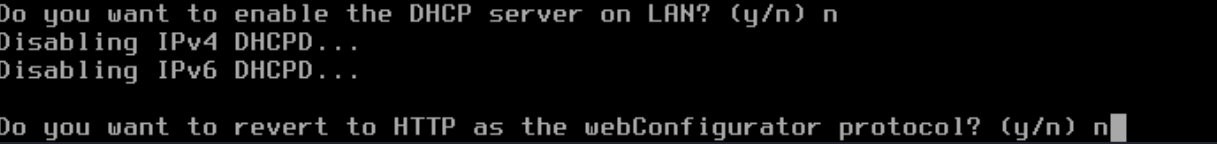


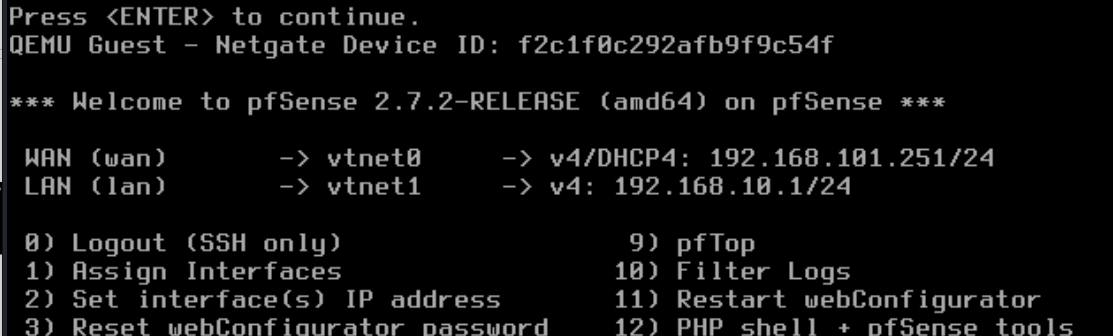


Maintenant on peut se connecte à l'interface web du pfsense a traver cette ip : 192.168.1.1

Mais reelement si on a fait ca dans une machine réelle ça va faire une collusion avec notre interface du routeur donc il faux mieux la changer

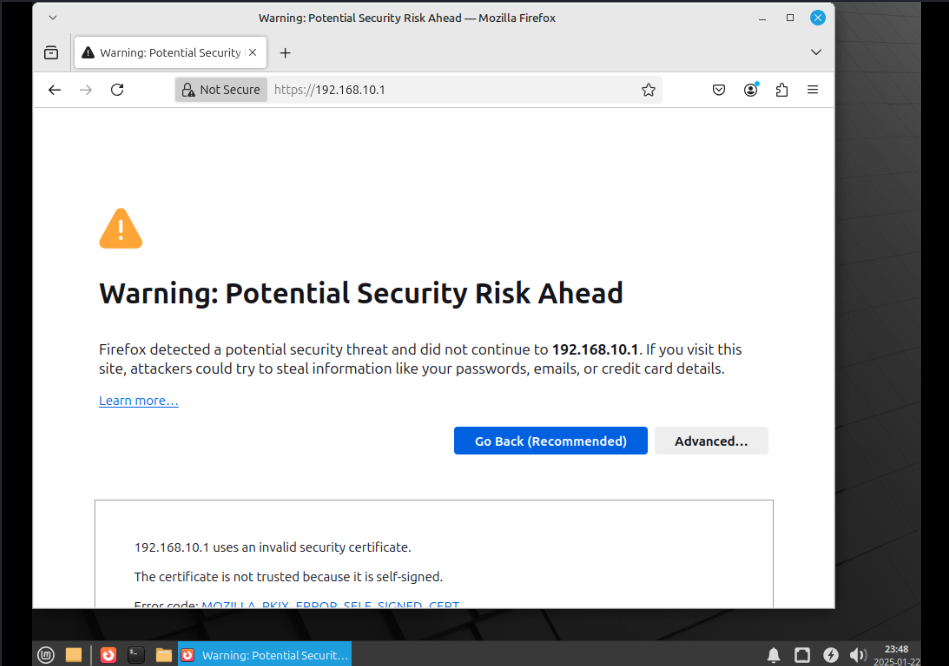




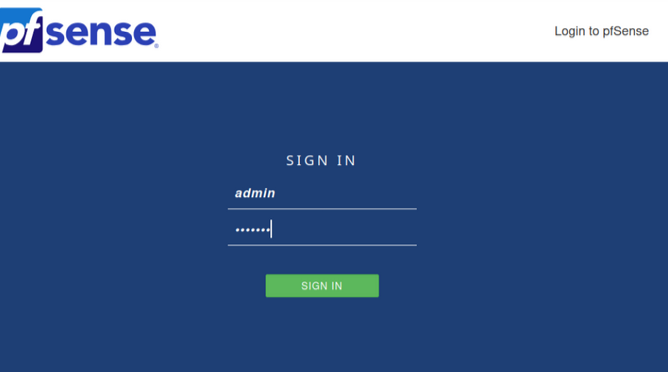


Maintenant tout est prêt.

Utilisant linux mint pour visiter l'interface web du pfsense

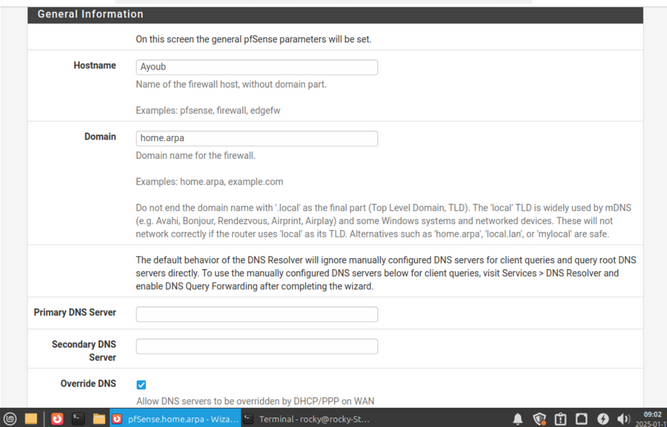


Utilisant le nom et mot passe par défaut : admin / pfsense

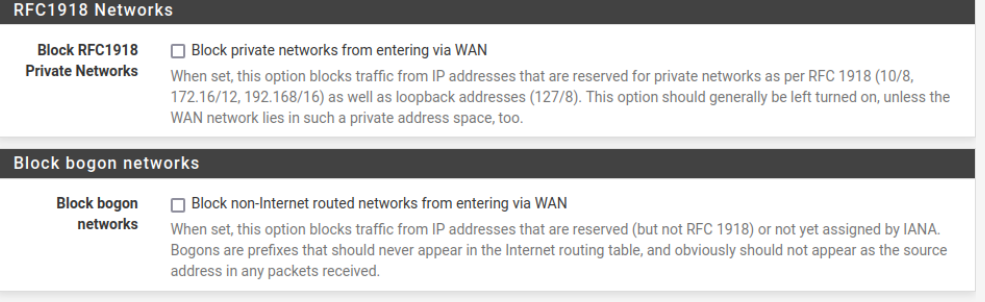


Hostname = nom du pare-feu

Domain : comme isetrades.com



On peut cocher ces deux options pour bloquer l’accès à notre réseau depuis Internet, c’est-à-dire le WAN



L’acces a internet possible :

