



REPUBLIQUE TUNISIENNE  
\*\*\*  
MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA  
RECHERCHE SCIENTIFIQUE  
\*\*\*\*\*  
DIRECTION GENERALE DES ETUDES  
TECHNOLOGIQUES  
\*\*\*\*\*  
Institut Supérieur des Etudes Technologiques de  
Radès



## 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 Abdennabi

**Année Universitaire :** 2024/2025

---

## **Remerciements**

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 fourni 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 Abdennabi, 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

<b>Chapitre 1 : Cadre du stage.....</b>	<b>7 - 12</b>
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 Objectifs 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](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

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 à 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.

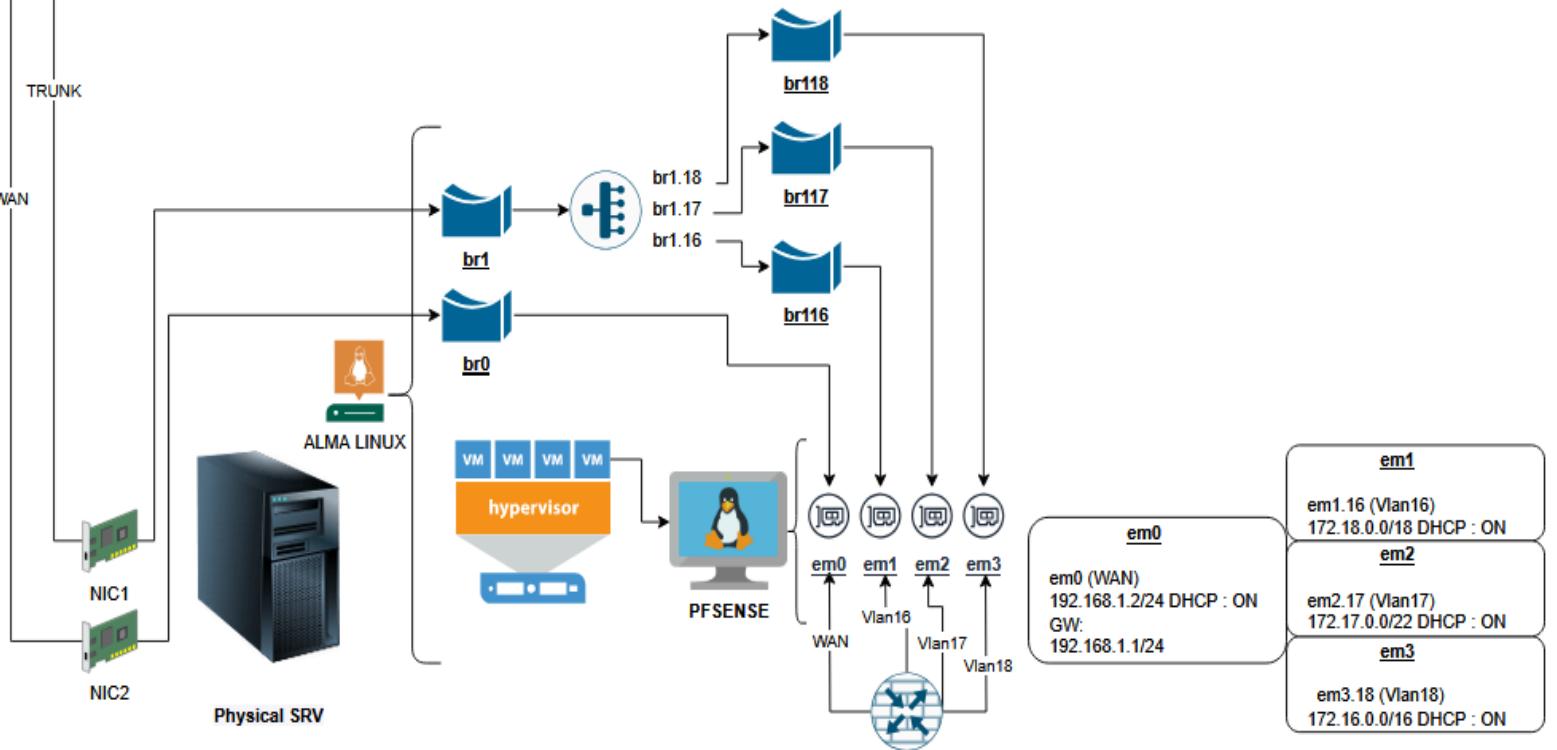
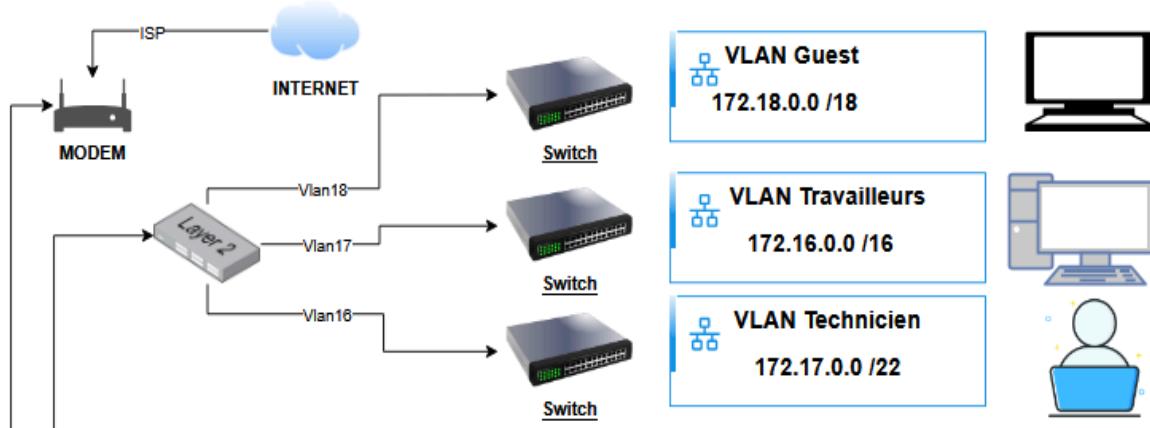
#### **Tests et validation :**

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.

## Interfaces / VLANs / Edit

### VLAN Configuration

<b>Parent Interface</b>	em1 (00:0c:29:4a:d7:6e) - lan
Only VLAN capable interfaces will be shown.	
<b>VLAN Tag</b>	100
802.1Q VLAN tag (between 1 and 4094).	
<b>VLAN Priority</b>	0
802.1Q VLAN Priority (between 0 and 7).	
<b>Description</b>	VLAN des Technicien
A group description may be entered here for administrative reference (not parsed).	
<b>Save</b>	

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

### General Configuration

<b>Enable</b>	<input checked="" type="checkbox"/> Enable interface	
<b>Description</b>	Guest	
Enter a description (name) for the interface here.		
<b>IPv4 Configuration Type</b>	Static IPv4	
<b>IPv6 Configuration Type</b>	None	
<b>MAC Address</b>	XXXX:XXXX:XXXX:XX	
The MAC address of a VLAN interface must be set on its parent interface		
<b>MTU</b>	<input type="text"/>	
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.		
<b>MSS</b>	<input type="text"/>	
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.		
<b>Speed and Duplex</b>	Default (no preference, typically autoselect)	
Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.		
<b>IPv4 Address</b>	172.15.0.1	/ 12

**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.

Firewall / Aliases / Edit

Properties	
Name	VLAN_Technicien The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	VLAN des Technicien A description may be entered here for administrative reference (not parsed).
Type	Network(s)
Network(s)	
Hint	Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.
Network or FQDN	192.168.128 / 25 Description Delete
<input type="button" value="Save"/> <input type="button" value="Add Network"/>	

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

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress. X

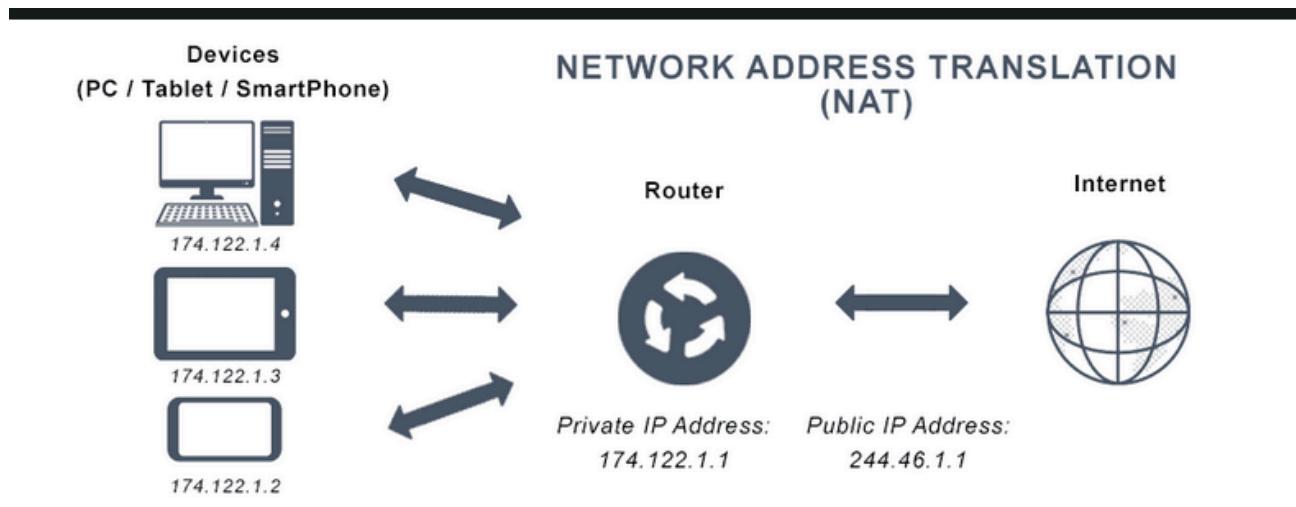
IP	Ports	URLs	All	
Firewall Aliases IP				
Name	Type	Values	Description	Actions
VLAN_Guest	Network(s)	172.18.0.0/18	VLAN des Guests	<input type="button" value="Edit"/> <input type="button" value="Import"/> <input type="button" value="Delete"/>
VLAN_Technicien	Network(s)	172.17.0.0/22	VLAN des Technicien	<input type="button" value="Edit"/> <input type="button" value="Import"/> <input type="button" value="Delete"/>
VLAN_Travailleurs	Network(s)	172.16.0.0/16	VLAN des Travailleurs	<input type="button" value="Edit"/> <input type="button" value="Import"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/> <input type="button" value="Import"/>				

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

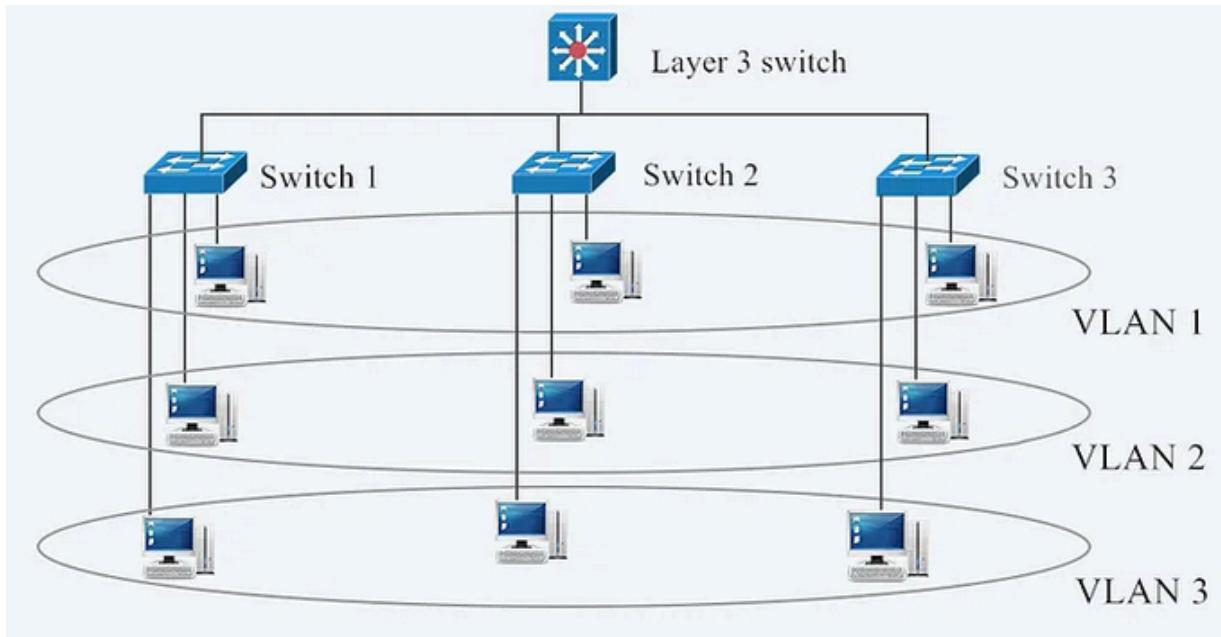
### 2.1.3 NAT/PAT et routage inter-VLAN avec le firewall

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.

Firewall / Traffic Shaper / Limiters

By Interface By Queue Limiters Wizards

**Limiters**

+ New Limiter

Enable  Enable limiter and its children

Name Limiteur VLAN Guest

Bandwidth	Bandwidth	Bw type	Schedule
10	Mbit/s	none	<span>Delete</span>

**Add Schedule**

Mask None

If "source" or "destination" slots is chosen a dynamic pipe with the bandwidth, delay, packet loss and queue size given above will be created for each source/destination IP address encountered, respectively. This makes it possible to easily specify bandwidth limits per host or subnet.

32	128
IPv4 mask bits 255.255.255.255/?	IPv6 mask bits ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/?

Description Limiteur Download/Upload pour le VLAN Guest

A description may be entered here for administrative reference (not parsed).

Figure 7: Crédit de la bande passante à 10 Mbps

## Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

## Source

Source Invert match

Address or Alias

VLAN\_Guest

/

## Destination

Destination Invert match

Any

Destination Address

/

▼

**Figure 8:** Sélection d'alias du VLAN Guest et tous les Protocols

## In / Out pipe

Limiteur\_VLAN\_Guest

Limiteur\_VLAN\_Guest\_

▼

Choose the Out queue/Virtual interface only if In is also selected. The Out selection is applied to traffic leaving the interface where the rule is created, the In selection is applied to traffic coming into the chosen interface.

If creating a floating rule, if the direction is In then the same rules apply, if the direction is Out the selections are reversed, Out is for incoming and In is for outgoing.

## Ackqueue / Queue

none

none

▼

Choose the Acknowledge Queue only if there is a selected Queue.

0/0 B

IPv4\*

VLAN\_Guest

\* \* \*

\* \* \*

none

Limiteur VLAN Guest

**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

**Edit Firewall Rule**

**Action:** Pass

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled:**  Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface:** WAN

Choose the interface from which packets must come to match this rule.

**Address Family:** IPv4

Select the Internet Protocol version this rule applies to.

**Protocol:** TCP

Choose which IP protocol this rule should match.

**Destination**

**Destination:**  Invert match Address or Alias VLAN\_Travailleurs

**Destination Port Range:** From: **HTTPS (443)** To: **HTTPS (443)** Custom Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Summary Bar: **0/0 B** IPv4 TCP \* \* **VLAN\_Travailleurs 443 (HTTPS)** \* none **anchor** **refresh** **undo** **trash**

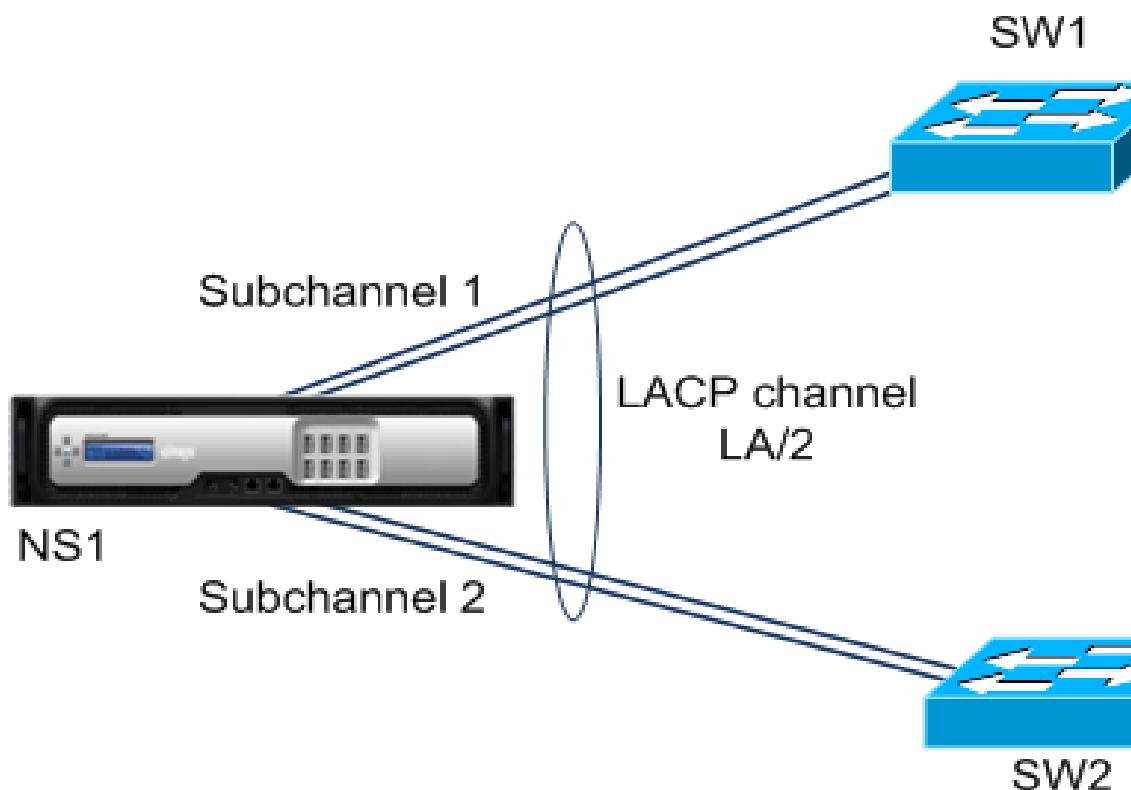
**Figure 10:** Création de règle de Pare-feu pour Tout Accès Entrant au Service HTTPS(Port 443) sous VLAN Travailleurs depuis le WAN + résultat

## 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 entre 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.

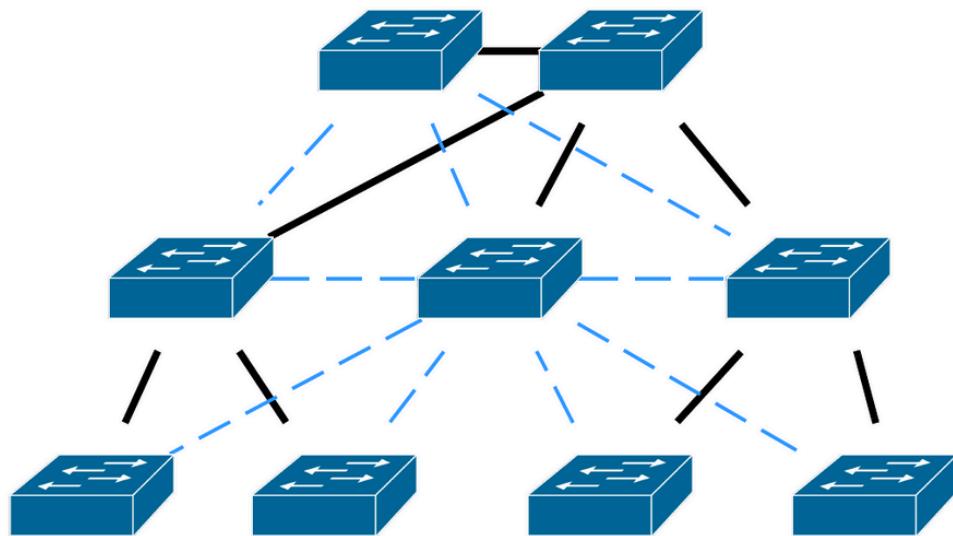
### **❖ Limitations de STP/RSTP/MSTP dans une topologie dual-switch**

- 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.

BGP et OSPF			
	BGP	OSPF	
Internet redundancy	Green	Red	Jamais/Rarrement
LAN	Red	Green	Toujours
WAN	Green	Yellow	Occasionnellement

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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term pfblockerng Both Search Clear

Enter a search string or \*nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
pfBlockerNG	3.2.0_8	Manage IPv4/v6 List Sources into 'Deny, Permit or Match' formats. GeoIP database by MaxMind Inc. (GeoLite2 Free version). De-Duplication, Suppression, and Reputation enhancements. Provision to download from diverse List formats. Advanced Integration for Proofpoint ET IQRisk IP Reputation Threat Sources. Domain Name (DNSBL) blocking via Unbound DNS Resolver.

Package Dependencies:

+ Install

lighttpd-1.4.72 jq-1.7\_1 gnugrep-3.11 rsync-3.2.7 py-maxminddb-2.4.0 libmaxminddb-1.7.1\_1 iprange-1.0.4 grepCIDR-2.0 python311-3.11.6 php82-8.2.11 php82-intl-8.2.11 py-sqlite3-3.11.6\_8

System / Package Manager / Package Installer

pfSense-pkg-pfBlockerNG installation successfully completed.

Installed Packages Available Packages Package Installer

Package Installation

```
https://bugs.freebsd.org/bugzilla  
More information about port maintainership is available at:  
https://docs.freebsd.org/en/articles/contributing/#ports-contributing  
=====  
Message from rsync-3.4.0:  
  
--  
Some scripts provided by rsync, such as rrsync,  
require Python, which is not installed by default.  
->>> Cleaning up cache... done.  
Success
```

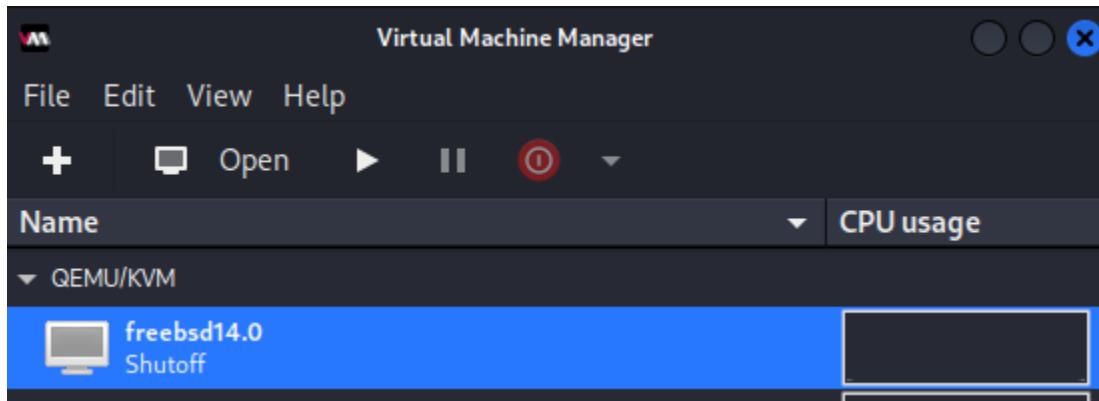
**Figure 14:** Installation du pfBlockerNG

## 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 général 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.

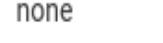
<input type="checkbox"/>	<span style="color: red;">X</span>	0/0 B	IPv4 TCP	TRAVAILLEURS subnets	*	*	*	*	none	
<input type="checkbox"/>	<span style="color: green;">✓</span>	0/0 B	IPv4 TCP	TRAVAILLEURS subnets	*	*	21 (FTP)	*	none	

**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.

<input type="checkbox"/>	<span style="color: green;">✓</span>	0/0 B	IPv4 TCP	TRAVAILLEURS subnets	*	*	21 (FTP)	*	none	
<input type="checkbox"/>	<span style="color: red;">X</span>	0/0 B	IPv4 TCP	TRAVAILLEURS subnets	*	*	*	*	none	

**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.

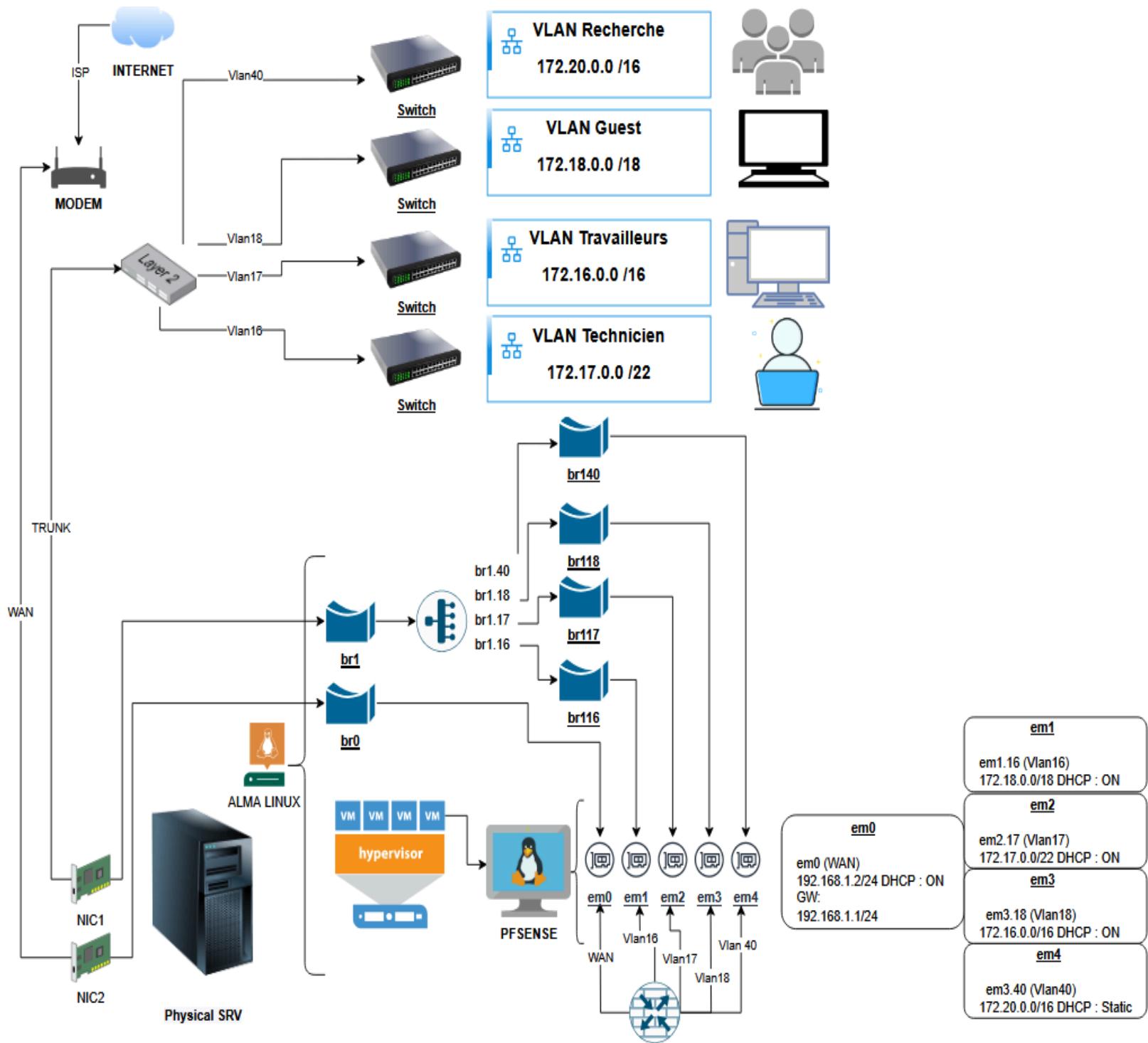
Interfaces / VLANs / Edit

### VLAN Configuration

<u>Parent Interface</u>	<input type="text" value="em2 (00:0c:29:4a:d7:78)"/> <b>L'interface à utiliser</b>
Only VLAN capable interfaces will be shown.	
<u>VLAN Tag</u>	<input type="text" value="40"/> <b>Tag / trunk</b>
802.1Q VLAN tag (between 1 and 4094).	
<u>VLAN Priority</u>	<input type="text" value="7"/> <b>Priorité QoS</b>
802.1Q VLAN Priority (between 0 and 7).	
<u>Description</u>	<input type="text" value="VLAN des Recherches"/>
A group description may be entered here for administrative reference (not parsed).	

**Save**

**Figure 18 :** Cration 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.

The screenshot shows the pfSense configuration interface for creating a new alias. The top navigation bar includes 'Firewall / Aliases / Edit'. The main window has a 'Properties' tab selected. In the 'Name' field, 'VLAN\_Internes' is entered. A note below states: 'The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".' The 'Description' field contains 'tous les VLAN (Guests , Travailleurs, Tehnicien )'. The 'Type' dropdown is set to 'Network(s)' and is highlighted with a red box. The 'Network(s)' tab is active, showing a table of configured networks. A 'Hint' note explains CIDR notation. Three entries are listed: '172.15.0.0 / 18 VLAN Guest', '172.16.0.0 / 16 VLAN Travailleurs', and '172.17.0.0 / 22 VLAN Technicien'. Each entry has a 'Delete' button to its right. At the bottom are 'Save', 'Export to file', and a green 'Add Network' button.

**Figure 20:** Crédit d'un Alias pour grouper tous les VLAN internes.

## Firewall / Rules / Edit

### Edit Firewall Rule

#### Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned whereas with block the packet is dropped silently. In either case, the original packet is discarded.

#### Disabled

Disable this rule

Set this option to disable this rule without removing it from the list.

#### Interface

RECH

Choose the interface from which packets must come to match this rule.

#### Address Family

IPv4

Select the Internet Protocol version this rule applies to.

#### Protocol

Any

Choose which IP protocol this rule should match.

### Source

#### Source

Invert match

RECH subnets

Source Address

### Destination

#### Destination

Invert match

Address or Alias

VLAN

VLAN\_Technicien

VLAN\_Travailleurs

VLAN\_Guest

VLAN\_Internes

### Extra Options

#### Log

Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot

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



## Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the source whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

## Source

Source Invert match

Address or Alias

VLAN\_Internes

## Destination

Destination Invert match

RECH subnets

Destination Address

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 *	VLAN_ Internes	*	! RECH subnets	*	*	none
--------------------------	-------------------------------------	-------	--------	----------------	---	----------------	---	---	------

**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.

The screenshot shows the 'General DHCP Options' section with the following settings:

- DHCP Backend: ISC DHCP
- Enable:  Enable DHCP server on RECH interface
- BOOTP:  Ignore BOOTP queries

In the 'Deny Unknown Clients' section, 'Allow all clients' is selected. A note explains: "When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to Allow known clients from **only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range."

In the 'Ignore Denied Clients' section, 'Ignore denied clients rather than reject' is unchecked. A note states: "This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured."

In the 'Ignore Client Identifiers' section, 'Do not record a unique identifier (UID) in client lease data if present in the client DHCP request' is unchecked. A note explains: "This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification."

The 'Primary Address Pool' section shows the following configuration:

- Subnet: 172.20.0.0/16
- Subnet Range: 172.20.0.1 - 172.20.255.254
- Address Pool Range: From 172.20.0.50 To 172.20.255.240

A note below the pool range states: "The specified range for this pool must not be within the range configured on any other address pool for this interface."

At the bottom, there is an 'Additional Pools' section with a green button labeled '+ Add Address Pool'.

**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.

General DNS Resolver Options						
Enable	<input checked="" type="checkbox"/> Enable DNS resolver					
Listen Port	53					
The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.						
Enable SSL/TLS Service	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.					
SSL/TLS Certificate	GUI default (679d40fb0a1af)					
The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.						
SSL/TLS Listen Port	853					
The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.						
<b>Network Interfaces</b>						
<table border="1"><tr><td>LAN</td></tr><tr><td>RECH</td></tr><tr><td>WAN IPv6 Link-Local</td></tr><tr><td>LAN IPv6 Link-Local</td></tr></table>		LAN	RECH	WAN IPv6 Link-Local	LAN IPv6 Link-Local	
LAN						
RECH						
WAN IPv6 Link-Local						
LAN IPv6 Link-Local						
Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.						
<b>Outgoing Network Interfaces</b>						
<table border="1"><tr><td>All</td></tr><tr><td>WAN</td></tr><tr><td>LAN</td></tr><tr><td>RECH</td></tr><tr><td>WAN IPv6 Link-Local</td></tr></table>		All	WAN	LAN	RECH	WAN IPv6 Link-Local
All						
WAN						
LAN						
RECH						
WAN IPv6 Link-Local						
Utilize different network interface(s) that the DNS Resolver will use to send queries to authoritative servers and receive their replies. By default all interfaces are used.						

<b>System Domain Local</b>	<input type="text" value="Transparent"/>
<b>Zone Type</b>	The local-zone type used for the pfSense system domain (System   General Setup   Domain). Transparent is the default.
<b>DNSSEC</b>	<input checked="" type="checkbox"/> Enable DNSSEC Support
<b>Python Module</b>	<input type="checkbox"/> Enable Python Module Enable the Python Module.
<b>DNS Query Forwarding</b>	<input type="checkbox"/> Enable Forwarding Mode  If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under <a href="#">System &gt; General Setup</a> or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).
	<input checked="" type="checkbox"/> Use SSL/TLS for outgoing DNS Queries to Forwarding Servers  When set in conjunction with DNS Query Forwarding, queries to all upstream forwarding DNS servers will be sent using SSL/TLS on the default port of 853. Note that ALL configured forwarding servers MUST support SSL/TLS queries on port 853.

**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)
<b>Méthode de résolution</b>	Résolution récursive locale	Redirige les requêtes vers des serveurs externes
<b>Sécurité</b>	Sécurisé avec DNSSEC et SSL/TLS	Dépend des serveurs en amont, moins sécurisé
<b>Dépendance externe</b>	Aucune, fonctionne de manière autonome	Dépend des serveurs DNS configurés
<b>Performance</b>	Peut être plus lent au premier accès mais efficace avec le cache	Plus rapide initialement mais moins sécurisé
<b>Utilisation des ressources</b>	Plus gourmand en CPU/RAM	Léger et rapide
<b>Utilisation recommandée</b>	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.

---

DNS Query Forwarding	<input type="checkbox"/> Enable Forwarding Mode
If this option is set, DNS queries will be forwarded to the upstream DNS servers defined under <a href="#">System &gt; General Setup</a> or those obtained via dynamic interfaces such as DHCP, PPP, or OpenVPN (if DNS Server Override is enabled there).	

**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.

```
[~] rhino-live@rhino-live $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    qlen 1000
        link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host noprefixroute
            valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    qlen 1000
        link/ether 00:0c:29:9a:6e:f3 brd ff:ff:ff:ff:ff:ff
        altname enp2s1
        inet 172.20.131.212/16 brd 172.20.255.255 scope global dynamic noprefixroute
    ens33
```

Leases							
	IP Address	MAC Address	Hostname	Description	Start	End	Actions
✓	192.168.1.101	00:50:56:c0:00:01	BRAFFLE		2025/02/01 21:25:01	2025/02/01 23:25:01	
✓	172.20.131.212	00:0c:29:9a:6e:f3	rhino-live		2025/02/01 21:23:41	2025/02/01 23:23:41	
✓	192.168.1.100	00:0c:29:9e:7a:7b	192.168.1.100		2025/02/01 21:12:44	2025/02/01 23:12:44	

Lease Utilization					
Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.1.100	192.168.1.199	2	100	2% of 100
RECH	172.20.0.50	172.20.255.240	1	65471	0% of 65471

**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.

## Diagnostics / Ping

?

### Ping

<u>Hostname</u>	<input type="text" value="8.8.8.8"/>
<u>IP Protocol</u>	<input type="text" value="IPv4"/>
<u>Source address</u>	<input type="text" value="RECH"/> Select source address for the ping.
<u>Maximum number of pings</u>	<input type="text" value="3"/> Select the maximum number of pings.
<u>Seconds between pings</u>	<input type="text" value="1"/> Select the number of seconds to wait between pings.

 Ping

### Results

```
PING 8.8.8.8 (8.8.8.8) from 172.20.0.1: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=113 time=122.694 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=66.469 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=53.498 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 53.498/80.887/122.694/30.033 ms
```

**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).
- Déetecter 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.

[System](#) [Firewall](#) [DHCP](#) [Authentication](#) [IPsec](#) [PPP](#) [PPPoE/L2TP Server](#) [OpenVPN](#) [NTP](#) [Packages](#) [Settings](#)[General](#) [Gateways](#) [Routing](#) [DNS Resolver](#) [Wireless](#) [GUI Service](#) [OS Boot](#)**Last 500 General Log Entries. (Maximum 500)**

Time	Process	PID	Message
Feb 1 12:36:59	kernel		XSAVE Features=0xf<XSAVEOPT,XSAVEC,XINUSE,XSAVES>
Feb 1 12:36:59	kernel		IA32_ARCH_CAPS=0x44<RSBA>
Feb 1 12:36:59	kernel		TSC: P-state invariant
Feb 1 12:36:59	kernel		Hypervisor: Origin = "VMwareVMware"
Feb 1 12:36:59	kernel		real memory = 1073741824 (1024 MB)
Feb 1 12:36:59	kernel		avail memory = 973459456 (928 MB)
Feb 1 12:36:59	kernel		Event timer "LAPIC" quality 600
Feb 1 12:36:59	kernel		ACPI APIC Table: <PTLTD APIC >
Feb 1 12:36:59	kernel		random: registering fast source Intel Secure Key RNG
Feb 1 12:36:59	kernel		random: fast provider: "Intel Secure Key RNG"
Feb 1 12:36:59	kernel		random: unblocking device.

**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.

Firewall / Aliases / Edit

Properties

Name	sites_reseaux_sociaux	The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".
Description	liens des reseaux sociaux	A description may be entered here for administrative reference (not parsed).
Type	Host(s)	

Host(s)

Hint		
Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.		
IP or FQDN	www.facebook.com	lien facebook
	www.instagram.com	lien instagram
	www.x.com	lien twitter

Figure 28 : Crédit d'alias des sites à bloquer

## Edit Firewall Rule

Action

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule

Set this option to disable this rule without removing it from the list.

**Interface**

Choose the interface from which packets must come to match this rule.

**Address Family**

Select the Internet Protocol version this rule applies to.

**Protocol**

Choose which IP protocol this rule should match.

## Source

**Source**  Invert match

The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

## Destination

**Destination**  Invert match

**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.

## Host Override Options

Host


Name of the host, without the domain part  
e.g.: "myhost"

Domain


Domain of the host  
e.g.: "example.com"

IP Address


IP address of the host  
e.g.: 192.168.100.100 or fd00:abcd::1

Description


A description may be entered here for administrative reference (not parsed).

## Additional Names for this Host



Delete



Delete

Host name

Domain

Description

Save
+ Add Host Name

**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 horaires

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.

## Schedule Information

**Schedule Name**

The name of the schedule may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description**

A description may be entered here for administrative reference (not parsed).

**Month**

**Date**

February_2025						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28		

Click individual date to select that date only. Click the appropriate weekday Header to select all occurrences of that weekday.

**Time**

Start Hrs

Start Mins

Stop Hrs

Stop Mins

Select the time range for the day(s) selected on the Month(s) above. A full day is 0:00-23:59.

**Time range description**

A description may be entered here for administrative reference (not parsed).

**+ Add Time**

**Clear selection**

## Configured Ranges

Day(s)

Start time

Stop time

Description

**Delete**

**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.

The screenshot shows the pfBlockerNG configuration page under the Firewall section. The top navigation bar includes links for General, IP, DNSBL, Update, Reports, Feeds, Logs, Sync, and Wizard. The General tab is selected. The main content area is titled "General Settings" and contains several configuration sections:

- Links**: Options for Firewall Aliases, Firewall Rules, and Firewall Logs.
- pfBlockerNG**: A section with a checked "Enable" checkbox. A note below it states: "Note: Context help is available on various pages by clicking the 'blue infoblock' icons" followed by a blue info icon.
- Keep Settings**: A section with a checked "Enable" checkbox. A note below it states: "Note: With 'Keep settings' enabled, pfBlockerNG will maintain run state on Installation/Upgrade. If 'Keep Settings' is not 'enabled' on pkg Install/De-Install, all settings will be Wiped!"
- CRON Settings**: A section for setting cron intervals. It includes dropdown menus for hour (Every hour), minute (00), start hour (0), and start minute (0). Below these are notes: "Default: Every hour Select the Cron hour interval.", "Default: :00 Select the Cron update minute.", "Default: 0 Select the Cron start hour.", and "Default: 0 Select the 'Daily/Weekly' start hour."
- Download Failure Threshold**: A section with a dropdown menu set to "No Limit". Notes below it state: "Default: No limit", "Select max daily download failure threshold via CRON. Clear widget 'failed downloads' to reset.", and "On a download failure, the previously downloaded list is reloaded."

**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.

The screenshot shows a web browser window with the title bar "pfSense.home.apra - Firefox" and the tab "Autonomous System Lookups". The URL in the address bar is "https://hackertarget.com/as-ip-lookup/". Below the address bar, there are links for "Rocky Linux", "Rocky Wiki", "Rocky Forums", "Rocky Mattermost", and "Rocky Reddit". The main header features the "HACKER TARGET" logo with a stylized "X" pattern above it, followed by navigation links for "SCANNERS", "TOOLS", "RESEARCH", "ASSESSMENTS", "ABOUT", and "CONTACT". On the right side of the header are "PRICING" and "LOG IN" buttons.

In the search bar, the word "twitter" is typed. Below the search bar is a teal button labeled "Lookup ASN".

The results section is titled "ASN Search Results". It includes a download link for an "xlsx" file and a search bar. The table displays the following data:

AS #	AS Name	AS Prefixes
13414	TWITTER, US	69.195.178.0/24 69.195.166.0/24 69.195.186.0/24 209.237.196.0/24 104.244.47.0/24 209.237.192.0/19 64.63.30.0/24 104.244.46.0/24 209.237.193.0/24

**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.

**IP Interface/Rules Configuration**

<b>Inbound Firewall Rules</b>	<input type="checkbox"/> WAN <input checked="" type="checkbox"/> LAN <small>Select the Inbound interface(s) you want to apply auto rules to:</small>	<input checked="" type="button"/> Block ▾ <small>Default: Block</small> <small>Select 'Rule action' for Inbound rules:</small>
<b>Outbound Firewall Rules</b>	<input type="checkbox"/> WAN <input checked="" type="checkbox"/> LAN <small>Select the Outbound interface(s) you want to apply auto rules to:</small>	<input checked="" type="button"/> Block ▾ <small>Default: Reject</small> <small>Select 'Rule action' for Outbound rules:</small>
<b>Floating Rules</b>	<input type="checkbox"/> Enable <small>Enabled: Auto-rules will be generated in the 'Floating Rules' tab.</small> <small>Disabled: Auto-rules will be generated in the selected Inbound/Outbound interfaces.</small>	
<b>Firewall 'Auto' Rule Order</b>	<input type="text" value="  pfB_Pass/Match/Block/Reject   All other Rules   (Default format)"/>	
	<small>Default Order:   pfB_Block/Reject   All other Rules   (original format)</small>	
	<small>Note: 'Auto type' Firewall Rules will be 'ordered' by this selection.</small>	
<b>Firewall 'Auto' Rule Suffix</b>	<input type="text" value="auto rule ▾"/> <small>Default: auto rule</small> <small>Select 'Auto Rule' description suffix for auto defined rules. pfBlockerNG must be disabled to modify suffix.</small>	
<b>Kill States</b>	<input type="checkbox"/> Enable <small>When 'Enabled', after a cron event or any 'Force' commands, any blocked IPs found in the Firewall states will be cleared.</small>	

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

IPv4    IPv6    GeoIP    Reputation

### Info

Links    Firewall Aliases    Firewall Rules    Firewall Logs

Name / Description	Resaux_Sociaux_BLOCK	Liste des reseaux sociaux a bloquer
Enter Name ( Max 24 characters ) and Description. <a href="#">i</a>		

### IPv4 Source Definitions

Format	State	Source	Header/Label	Delete
ASN	ON	AS32934 [ FACEBOOK, US ]	AS32934	<a href="#">Delete</a>
ASN	ON	AS63293 [ FACEBOOK-OFFNET, US ]	AS63293	<a href="#">Delete</a>
ASN	ON	AS13414 [ TWITTER, US ]	AS13414	<a href="#">Delete</a>

Click here for Guidelines --> [i](#)

[+ Add](#)    [Enable All](#)

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

### Settings

Action	Deny Outbound	Default: Disabled For Non-Alias type rules you must define the appropriate Firewall 'Auto' Rule Order option. Click here for more info --> <a href="#">i</a>
Update Frequency	Every 12 hours	Default: Never Select how often List files will be downloaded. This must be within the Cron Interval/Start Hour settings.
Weekly (Day of Week)	Monday	Default: Monday Select the 'Weekly' ( Day of the Week ) to Update This is only required for the 'Weekly' Frequency Selection. The 24 Hour Download 'Time' will be used.
Auto-Sort Header field	Enable auto-sort	Automatic sorting of the Header/Label field grouped by the Enabled/Disabled State field setting.
Enable Logging	Enabled	Default: Enable Select - Logging to Status: System Logs: FIREWALL ( Log ) This can be overridden by the 'Global Logging' Option in the General Tab.
States Removal	Enabled	With the 'Kill States' option (General Tab), you can disable States removal for this Alias.

**Figure 35 :** Configuration des paramètres

- Cette Figure montre la configuration des paramètres de la règle de 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.

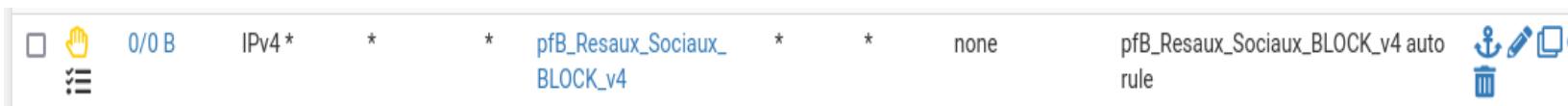
❖ Pour appliquer les modifications et télécharger les listes mises à jour, il est nécessaire de se rendre dans l'onglet Update de pfBlockerNG et de cliquer sur Run. Cette action permet de récupérer et d'installer les listes définies, assurant ainsi un filtrage efficace selon les règles configurées.

The screenshot shows the pfBlockerNG interface with the following details:

- Header:** Firewall / pfBlockerNG / Update
- Menu Bar:** General, IP, DNSBL, **Update**, Reports, Feeds, Logs, Sync
- Section Header:** Update Settings
- Links:** Firewall Aliases, Firewall Rules, Firewall Logs
- Status:** NEXT Scheduled CRON Event will run at 13:00 with 00:06:25 time remaining. Refresh to update current status and time remaining.
- Force Options:** \*\* AVOID \*\* Running these "Force" options - when CRON is expected to RUN! (with an information icon)
- Select 'Force' option:** Radio buttons for Update (selected), Cron, and Reload.
- Buttons:** Run (highlighted with a red box), View

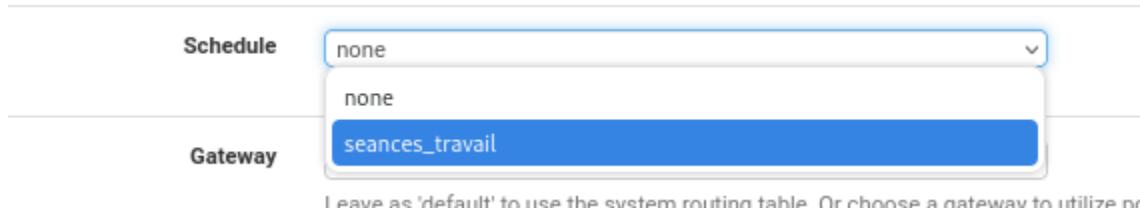
**Figure 36:** Exécution de la mise à jour des listes dans pfBlockerNG

- ❖ 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

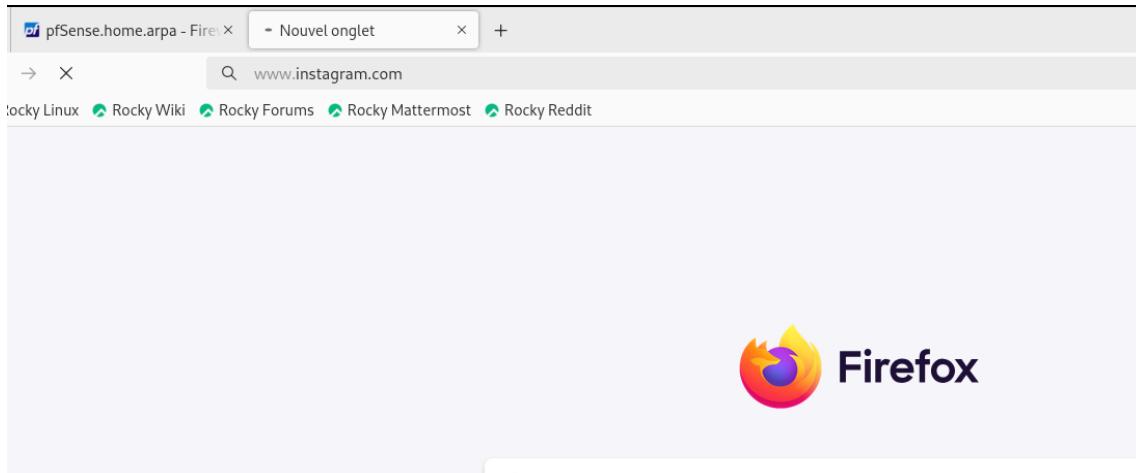
---

# 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.

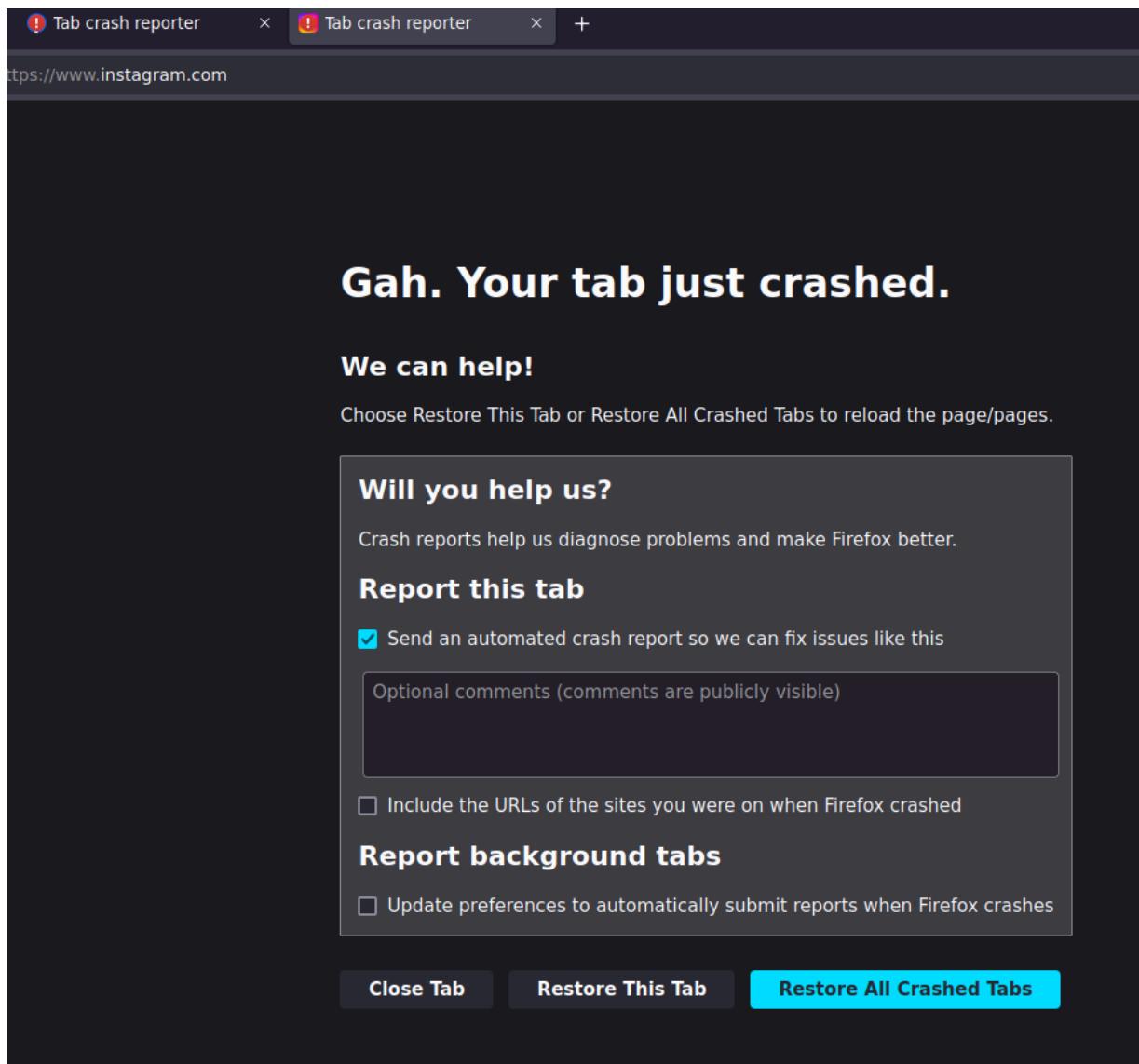
### 5.1.2. Problèmes rencontrés et solutions pour éviter les échecs

- ❖ 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.

**Interface** LAN Choose the interface from which packets must come to match this rule.

**Address Family** IPv4 Select the Internet Protocol version this rule applies to.

**Protocol** TCP/UDP Choose which IP protocol this rule should match.

**Source**

<b>Source</b>	<input type="checkbox"/> Invert match	Address or Alias	VLAN_Internes
---------------	---------------------------------------	------------------	---------------

**Destination**

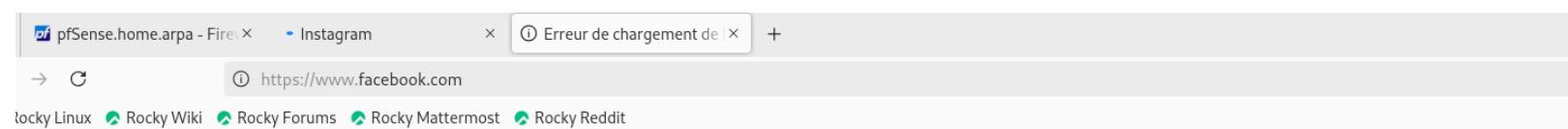
<b>Destination</b>	<input type="checkbox"/> Invert match	LAN address	Destination Address	
<b>Destination Port Range</b>	From: DNS (53)	Custom	To: DNS (53)	Custom

**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.

```
(ayoub@study)-[~]$ sudo apt install qemu-kvm libvirt-clients libvirt-daemon-system bridge-utils
Note, selecting 'qemu-system-x86' instead of 'qemu-kvm'
qemu-system-x86 is already the newest version (1:9.2.0+ds-2).
libvirt-clients is already the newest version (10.10.0-3).
libvirt-daemon-system is already the newest version (10.10.0-3).
bridge-utils is already the newest version (1.7.1-3).
```

**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).

```
(ayoub@study)-[~]$ sudo adduser ayoub libvirt && sudo adduser ayoub libvirt
[sudo] password for ayoub:
info: Adding user `ayoub' to group `libvirt' ...
info: The user `ayoub' is already a member of `libvirt'.
```

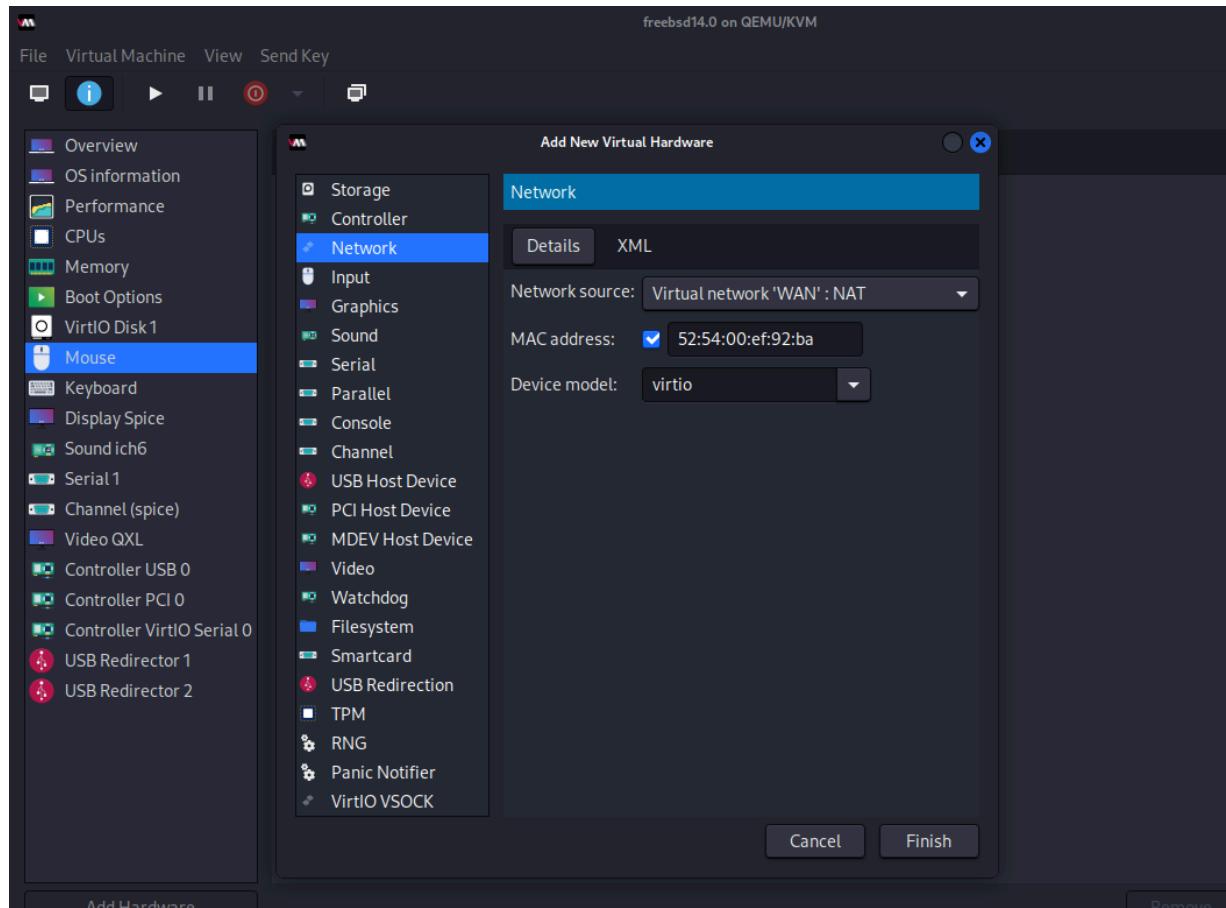
**CMD:** sudo apt install virt-manager

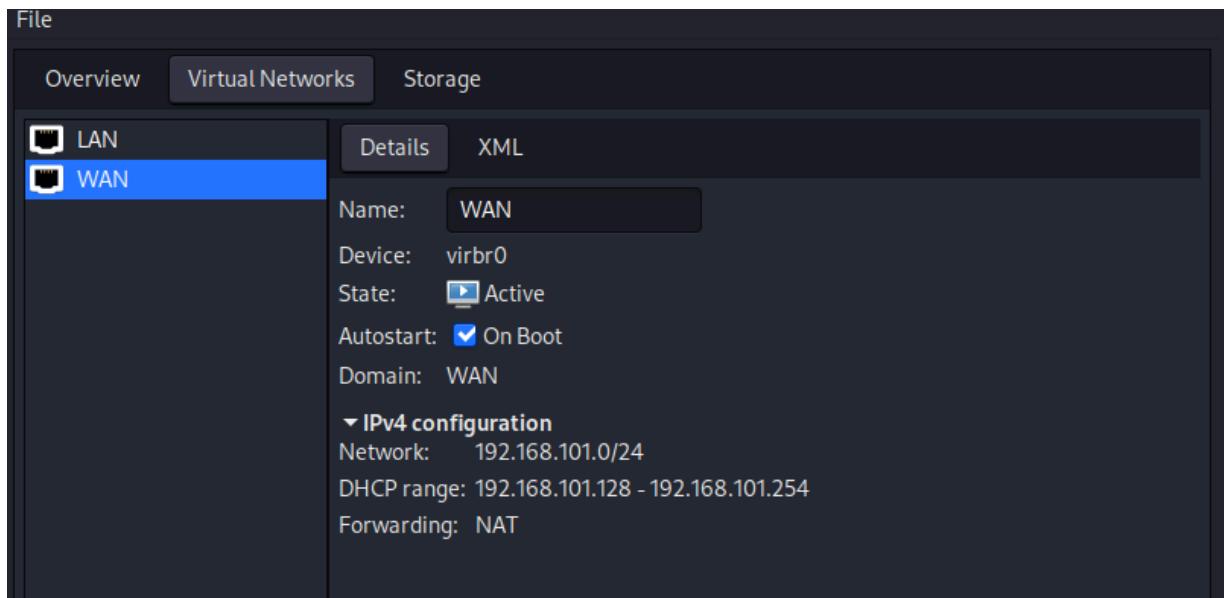
Cette commande permet d'installer virt-manager, un outil graphique pour gérer des machines virtuelles avec KVM/QEMU.

```
(ayoub@study) [~]$ sudo apt install virt-manager
virt-manager is already the newest version (1:5.0.0-3).
The following packages were automatically installed and
```

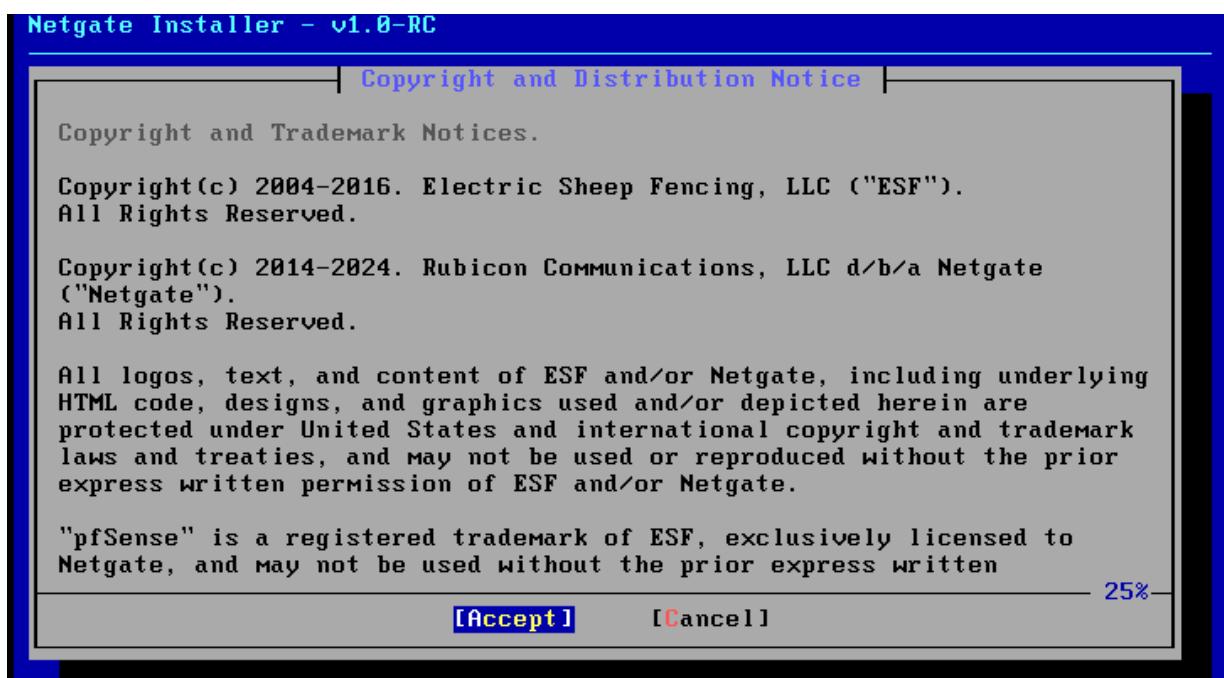
## pfSense Setup

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 :

```
pkg-static: Warning: Major OS version upgrade detected. Running "pkg boot
Updating pfSense-core repository catalogue...
Fetching meta.conf: . done
Fetching packagesite.pkg: . done
Processing entries: . done
pfSense-core repository update completed. 4 packages processed.
Updating pfSense repository catalogue...
Fetching meta.conf: . done
Fetching data.pkg: ..... done
Processing entries: ..... done
pfSense repository update completed. 550 packages processed.
All repositories are up to date.
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  pkg: 1.20.8_3 [pfSense]

Number of packages to be installed: 1

The process will require 39 MiB more space.
10 MiB to be downloaded.
```

On est face à ce console :

```
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y\ln]? 2025-01-22T23:15:38.446536+00:00 - php-fpm 397
-- /rc.linkup: Ignoring link event during boot sequence.
2025-01-22T23:15:38.451351+00:00 - php-fpm 625 -- /rc.linkup: Ignoring link eve
nt during boot sequence.

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtinet0 vtinet1 or a):
```

Il est toujours mieux de double check les cartes Utilisant :

- Ip a

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

```
valid_lft forever preferred_lft forever
7: virbr0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc htb state UP group default qlen 1
    link/ether 52:54:00:7e:bf:34 brd ff:ff:ff:ff:ff:ff
      inet 192.168.101.1/24 brd 192.168.101.255 scope global virbr0
        valid_lft forever preferred_lft forever
8: virbr1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc htb state UP group default qlen 1
    link/ether 52:54:00:f5:83:03 brd ff:ff:ff:ff:ff:ff
      inet 192.168.10.1/24 brd 192.168.10.255 scope global virbr1
        valid_lft forever preferred_lft forever
9: vnet0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master virbr0 state UNKNOWN
10: vnet1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master virbr1 state UNKNOWN
    link/ether fe:54:00:ef:92:ba brd ff:ff:ff:ff:ff:ff
      inet6 fe80::fc54:ff:feef:92ba/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
11: vnet2: <NOQUEUE,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master virbr1 state UNKNOWN
    link/ether fe:54:00:6d:18:1f brd ff:ff:ff:ff:ff:ff
      inet6 fe80::fc54:ff:fe6d:181f/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
```

Puis on va compléter la configuration via console:

```
Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 a or nothing if finished): vtnet1

The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1

Do you want to proceed [y\ln]? y
```

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

QEMU Guest - Netgate Device ID: f2c1f0c292afb9f9c54f

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.101.251/24
LAN (lan)      -> vtnet1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell
```

Maintenant on peut se connecter à l'interface web du pfsense à travers cette ip :  
192.168.1.1

Mais reélement si on a fait ça dans une machine réelle ça va faire une collision avec notre interface du routeur donc il faut mieux la changer

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - dhcp)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.10.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
> █
```

```
Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

```
Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: f2c1f0c292afb9f9c54f

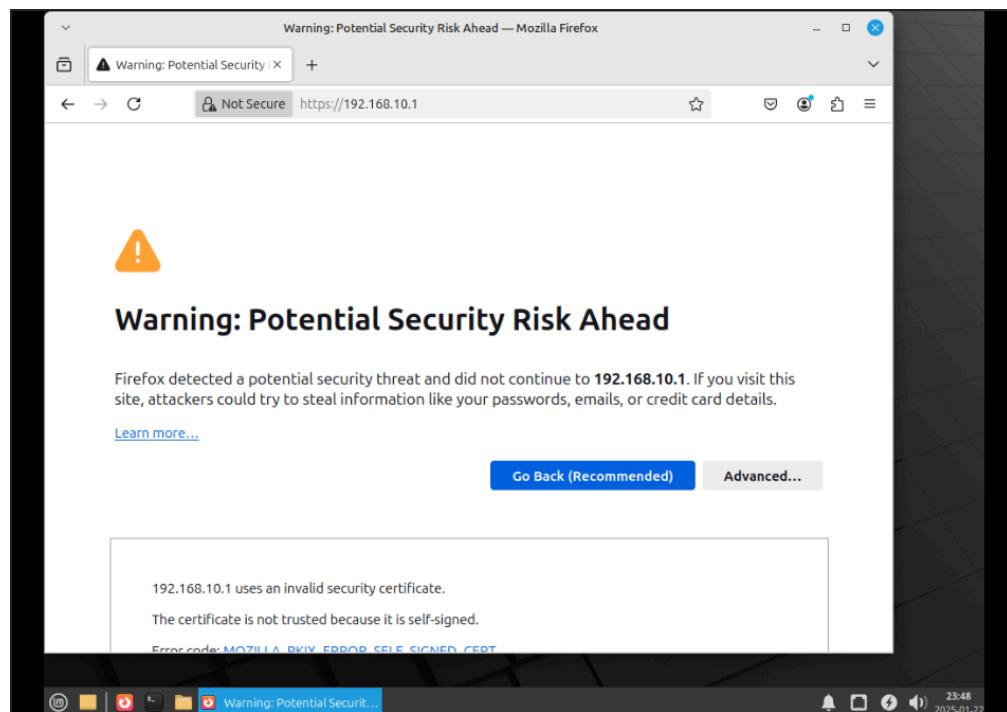
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtne0       -> v4/DHCP4: 192.168.101.251/24
LAN (lan)      -> vtne1       -> v4: 192.168.10.1/24

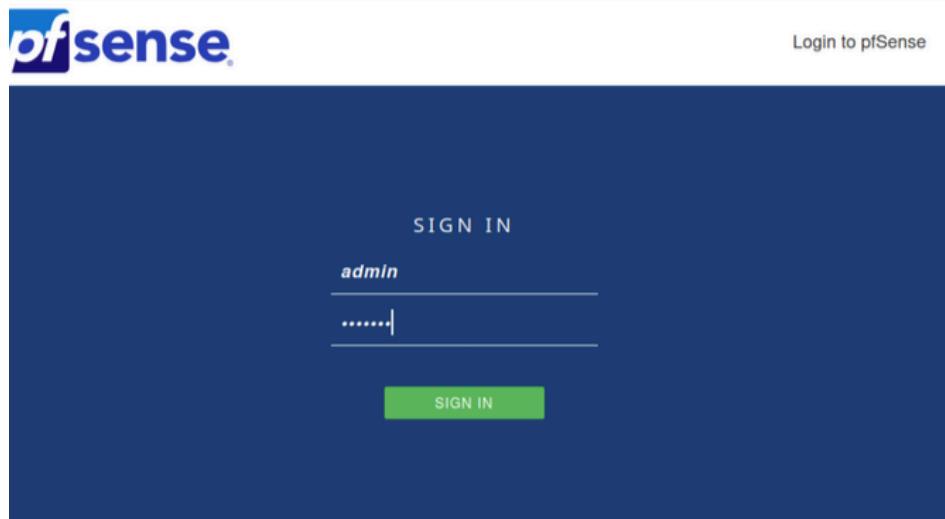
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
```

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

**General Information**

On this screen the general pfSense parameters will be set.

<b>Hostname</b>	Ayoub
Name of the firewall host, without domain part.	
Examples: pfsense, firewall, edgefw	
<b>Domain</b>	home.arpa
Domain name for the firewall.	
Examples: home.arpa, example.com	
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.	
The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.	
<b>Primary DNS Server</b>	<input type="text"/>
<b>Secondary DNS Server</b>	<input type="text"/>
<b>Override DNS</b>	<input checked="" type="checkbox"/>
Allow DNS servers to be overridden by DHCP/PPP on WAN	

pfSense.home.arpa - Wiz... Terminal - rocky@rocky-St... 09:02 2024-01-11

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

### RFC1918 Networks

- Block RFC1918 Private Networks**  Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). This option should generally be left turned on, unless the WAN network lies in such a private address space, too.

### Block bogon networks

- Block bogon networks**  Block non-Internet routed networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets received.

L'accès à internet possible :

A screenshot of a web browser window displaying the English Wikipedia homepage. The address bar shows the URL <https://www.wikipedia.org>. The page title is "WIKIPEDIA" with the subtitle "L'encyclopédie libre". Below the title, there are links to other language versions: Français (2 659 000+ articles), English (6,942,000+ articles), 日本語 (1,445,000+記事), Deutsch (2.979.000+ Artikel), Italiano (1.900.000+ voci), فارسی (۱۰۰.۰۰۰+ مقاله), Русский (2 020 000+ статей), Español (2.003.000+ artículos), 中文 (1,459,000+ 条目 / 修目), and Polski (1 645 000+ haszel). A central feature is the iconic Wikipedia logo, a globe composed of puzzle pieces with various symbols on them. At the bottom, there is a search bar with the text "FR" and a magnifying glass icon.