THEME: Supervision Réseau avec pfSense

Auteurs

WATO MABOU PAUL 22T2920
MASSE MASSE PAUL-BASTHYLLE 22U2001

Sous la supervision de

Dr. DOMGA et Mr. NGUANFO

Contents

Introduction

La supervision réseau joue un rôle essentiel dans la gestion moderne des infrastructures informatiques. Elle permet non seulement de surveiller la performance d'un réseau, mais aussi de détecter et prévenir des pannes, des intrusions ou des dysfonctionnements avant qu'ils n'affectent la productivité. Dans un contexte où la sécurité et la disponibilité du réseau sont primordiales, il est impératif d'utiliser des outils fiables et robustes.

Ce rapport se concentre sur l'utilisation de pfSense, une solution open-source basée sur le système d'exploitation FreeBSD, reconnue pour sa polyvalence et sa fiabilité. Nous explorerons dans ce document les principales fonctionnalités de pfSense, son installation et sa configuration à travers des tests concrets tels que la création d'un portail captif, la gestion de la bande passante avec le Traffic Shaper, et la mise en place de Stress Testing afin de garantir une gestion optimale des ressources du réseau.

Chapter 1

Présentation de pfSense et Fonctionnalités

1.1 Présentation de l'outil

1.1.1 Description générale

pfSense est une distribution logicielle de pare-feu/routeur basée sur FreeBSD. Les versions open source pfSense Community Edition (CE) et pfSense Plus peuvent être installées sur un ordinateur physique ou une machine virtuelle pour créer un pare-feu/routeur dédié à un réseau. Il peut être configuré et mis à niveau via une interface web, ne nécessitant aucune connaissance préalable du système FreeBSD sous-jacent.

pfSense est conçu pour offrir des fonctionnalités de pare-feu et de routage robustes, adaptées à divers environnements, des petites entreprises aux grandes infrastructures.

1.1.2 Historique

Le projet pfSense a débuté en 2004 en tant que fourchette du projet m0n0wall, initié par Chris Buechler et Scott Ullrich. Sa première version est sortie en octobre 2006. Le nom pfSense provient de l'utilisation de l'outil de filtrage de paquets PF.

En janvier 2015, OPNsense a été lancé comme une fourche parallèle de pfSense. En novembre 2017, l'Organisation mondiale de la propriété intellectuelle a constaté que Netgate, détenteur des droits d'auteur de pfSense, avait utilisé les marques déposées d'OPNsense de mauvaise foi pour discréditer ce dernier et a ordonné à Netgate de transférer un nom de domaine à Deciso.

En février 2021, pfSense CE 2.5.0 et pfSense Plus 21.02 ont ajouté le support de WireGuard. Cependant, cette fonctionnalité a été temporairement retirée en mars 2021 en raison de problèmes d'implémentation découverts par Jason Donenfeld, le fondateur de WireGuard. La version 2.5.2 de pfSense CE de juillet 2021 a réintégré WireGuard.

1.1.3 Utilité

pfSense s'adapte aussi bien aux réseaux domestiques qu'aux grandes entreprises. Il est particulièrement efficace pour les infrastructures nécessitant une surveillance de sécurité avancée et une gestion optimisée du trafic réseau, incluant plusieurs sous-réseaux et des connexions VPN.

1.1.4 Version, licence, exigences et taille de l'infrastructure

Actuellement, pfSense dispose de plusieurs versions : 1.2.X, 2.0.X, 2.1.X, 2.2.X, 2.3.X, 2.4.X, 2.5.X, 2.6.X, 2.7.X.

Il utilise une licence Apache 2.0 et son installation nécessite les spécifications suivantes :

- 64-bit amd64 (x86-64) compatible CPU
- 1GB or more RAM
- 8 GB or larger disk drive (SSD, HDD, etc.)
- One or more compatible network interface cards

1.1.5 Interface web intuitive

pfSense offre une interface web intuitive pour la gestion réseau et la configuration des règles de pare-feu.

1.1.6 Utilisation dans les réseaux

Utilisation dans des réseaux de petite, moyenne ou grande taille.

1.2 Fonctionnalités de pfSense

1.2.1 Fonctionnalités clés

Surveillance des ressources système

pfSense propose des outils de surveillance en temps réel de la CPU, de la mémoire et de la bande passante. Cette fonctionnalité aide à identifier rapidement les goulets d'étranglement et à maintenir la performance du réseau.

Gestion des alertes et notifications

Les alertes peuvent être configurées pour notifier les administrateurs en cas d'événements critiques, assurant ainsi une réactivité immédiate en cas de surcharge ou de tentative d'intrusion.

Génération de rapports

pfSense permet de générer des rapports détaillés sur le trafic réseau, les tentatives d'accès et les performances. Ces rapports facilitent l'analyse rétrospective et l'optimisation du réseau.

Surveillance en temps réel du trafic réseau

La surveillance en temps réel du trafic réseau suit l'activité, détecte les anomalies (bande passante, connexions non autorisées) et offre des outils visuels via l'interface de pfSense pour une analyse rapide.

1.2.2 Fonctionnalités supplémentaires

- **Pare-feu et NAT avancés** : Permet un contrôle précis du trafic réseau avec des règles personnalisées et la traduction d'adresses réseau pour connecter des sous-réseaux.
- **Routage avancé** : Prend en charge le routage statique et dynamique, ainsi que l'équilibrage de charge pour optimiser le trafic entre plusieurs chemins.
- **VPN (OpenVPN, IPsec, etc.)** : Offre des connexions sécurisées entre différents réseaux ou utilisateurs distants grâce à des protocoles de tunnels chiffrés.
- **Filtrage de contenu** : Bloque ou restreint l'accès à certains sites ou contenus grâce à des listes noires ou des règles de filtrage.
- **Haute disponibilité** : Assure une redondance réseau en basculant automatiquement sur une autre machine en cas de défaillance.
- **Gestion de la bande passante** : Priorise certains types de trafic pour garantir une utilisation efficace des ressources réseau.
- **Génération de rapports et journaux** : Enregistre et analyse l'activité réseau pour diagnostiquer les problèmes et assurer un suivi.

1.2.3 Fonctionnalités de sécurité

Portail captif

Le portail captif permet de contrôler l'accès réseau. Des utilisateurs peuvent être créés avec des droits restreints et gérés via un tableau de bord.

Règles de pare-feu

Des règles de pare-feu peuvent être configurées pour autoriser ou restreindre l'accès entre les VLANs, assurant un contrôle strict du trafic.

Limitation des connexions

pfSense permet de limiter les connexions simultanées, par exemple en autorisant un maximum de 4 connexions entre certains VLANs.

Chapter 2

Installation et Initialisation de pfSense

2.1 Téléchargement de l'image ISO

Pour installer pfSense, téléchargez l'image ISO depuis son site officiel. Vous pouvez la télécharger sur le lien suivant : `https://www.pfsense.org/download`.

(par exemple, « pfSense-CE-2.7.0-RELEASE-amd64.iso »).

- **Site officiel** : Téléchargez l'image ISO depuis le site officiel de pfSense.
- **Netgate** : Téléchargement directement depuis Netgate (payant).
- **Contournement des restrictions** : Utilisez des commandes pour contourner les restrictions.
- **Tuto étudiant** : Un tutoriel où les étudiants faisaient des tests et ont laissé un lien pour télécharger gratuitement.

2.2 Installation de VirtualBox

Installez VirtualBox pour créer une machine virtuelle.

2.3 Configuration de la VM

Configurez la machine virtuelle avec au moins :

- 1 Go de RAM
- 8 Go de stockage
- Une carte réseau en mode NAT ou en réseau interne

2.4 Paramètres réseau

Configurez les options réseau en choisissant l'un des modes suivants :

- Réseau interne

- NAT
- Accès par pont

2.5 Lancer la VM

2.5.1 VM Lubuntu

Configuration de la machine virtuelle Lubuntu, puis suivez les instructions.

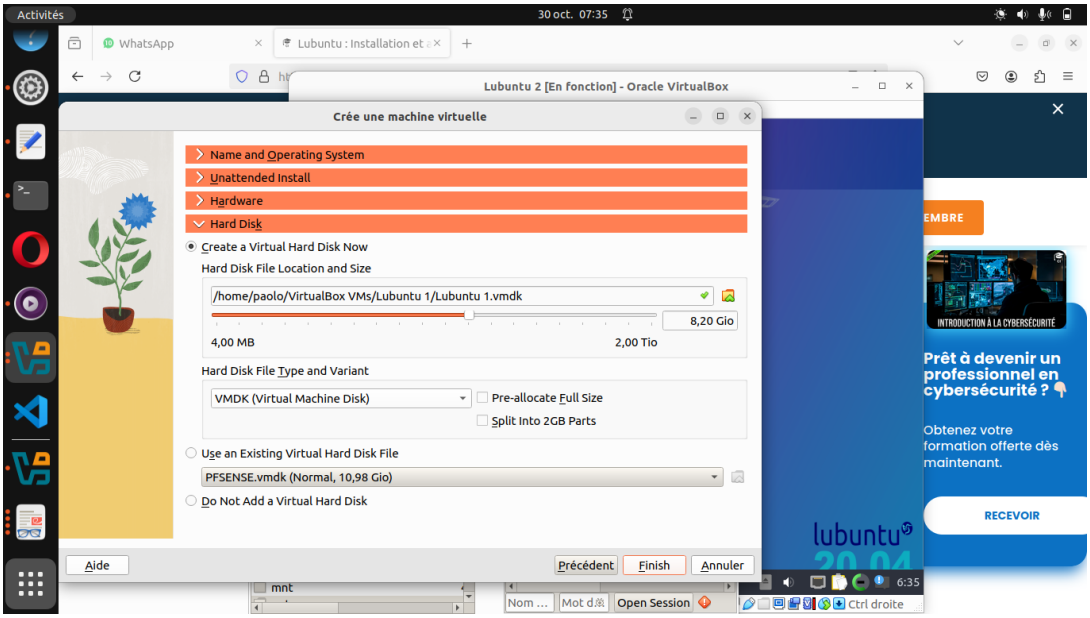


Figure 2.1: Configuration de la machine virtuelle Lubuntu.

2.5.2 Installer pfSense

Démarrez la machine virtuelle et suivez les instructions pour installer pfSense.

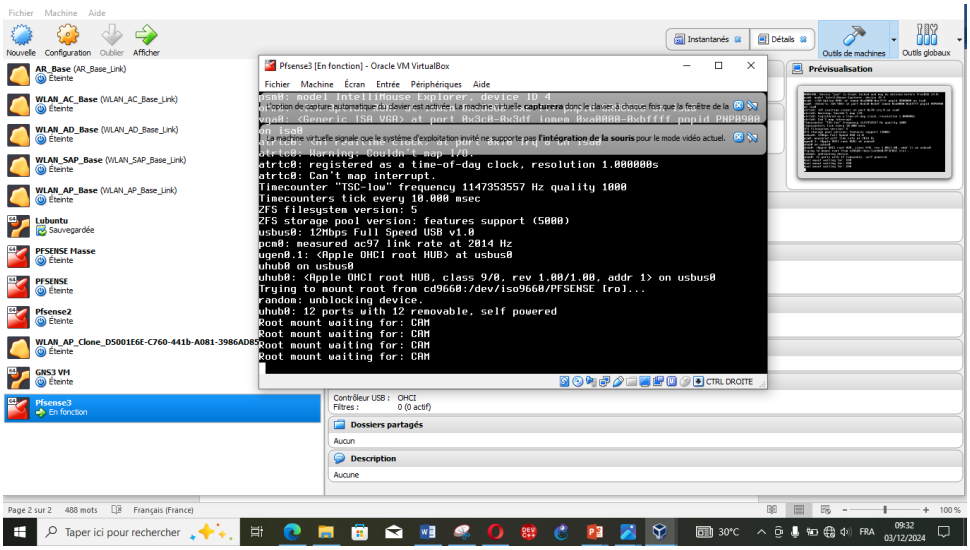


Figure 2.2: Installation de pfSense.

2.5.3 Reboot

Redémarrez la machine virtuelle après l'installation de pfSense.

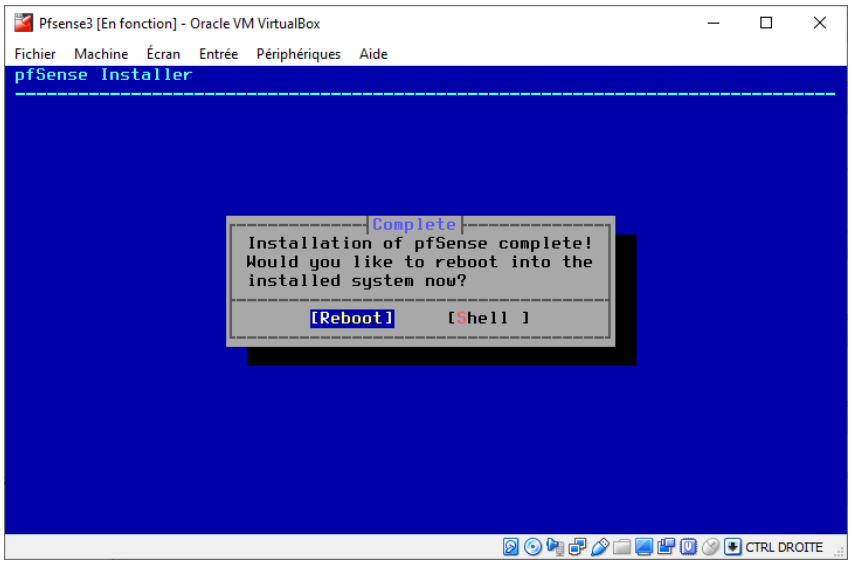


Figure 2.3: Redémarrage après installation de pfSense.

2.6 Accéder à l'interface de pfSense

2.6.1 Configuration de l'interface LAN

Après avoir affiché les options de pfSense :

1. Appuyez sur la touche **2**
2. Appuyez sur la touche **2** pour sélectionner l'option **LAN**.
3. Choisissez **DHCP** ou entrez une configuration manuelle.
4. Si vous choisissez **Manuel** :
   - Entrez l'adresse IP.
   - Configurez le masque de sous-réseau.

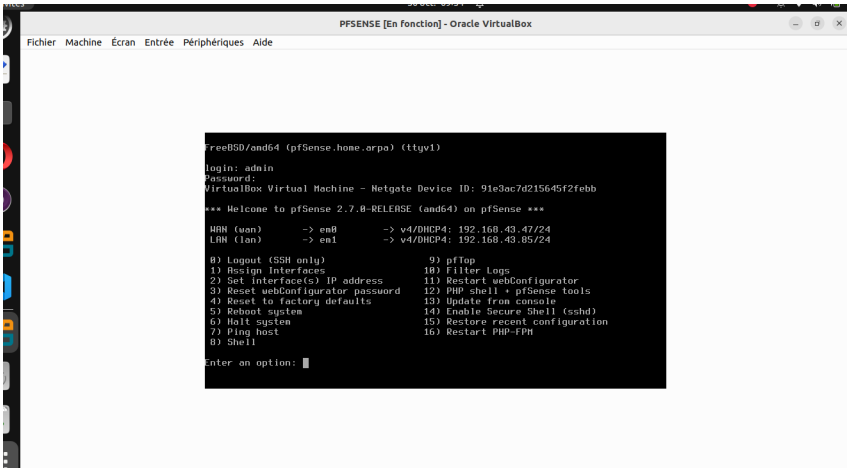


Figure 2.4: Interface pfSense.

2.6.2 Accéder à l'interface graphique via le navigateur

Pour accéder à l'interface graphique de pfSense :

- Ouvrez un navigateur web.
- Entrez l'adresse IP de pfSense dans la barre d'adresse.
- Identifiez-vous avec :
  - **Login** : `admin`
  - **Mot de passe** : `pfsense` (par défaut)

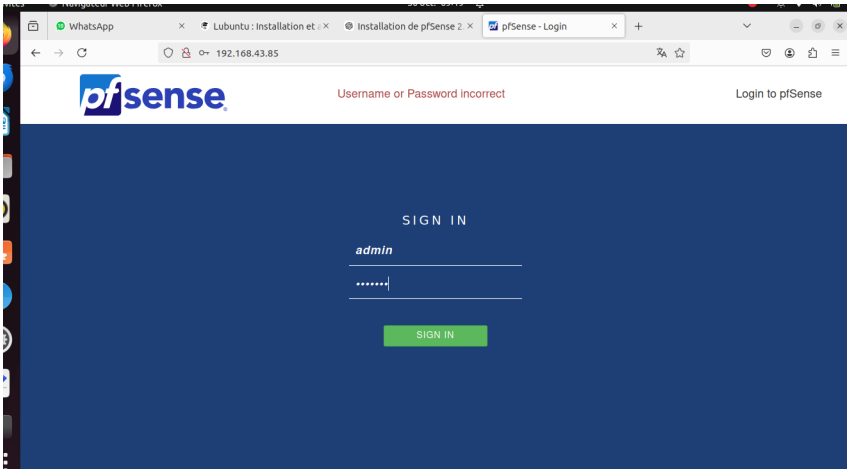


Figure 2.5: Interface d'authentification pfSense.

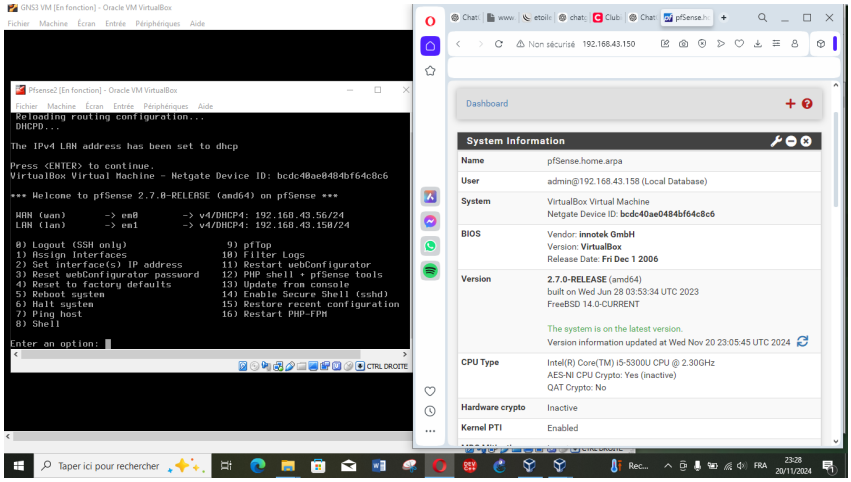


Figure 2.6: interface graphique sur Machine hôte

2.6.3 Exemple avec une autre VM (Ex : Lubuntu)

- Assurez-vous que la VM est connectée au même réseau que pfSense.
- Utilisez un navigateur installé sur Lubuntu pour accéder à l'interface.

2.6.4 Résultat

On obtient alors:

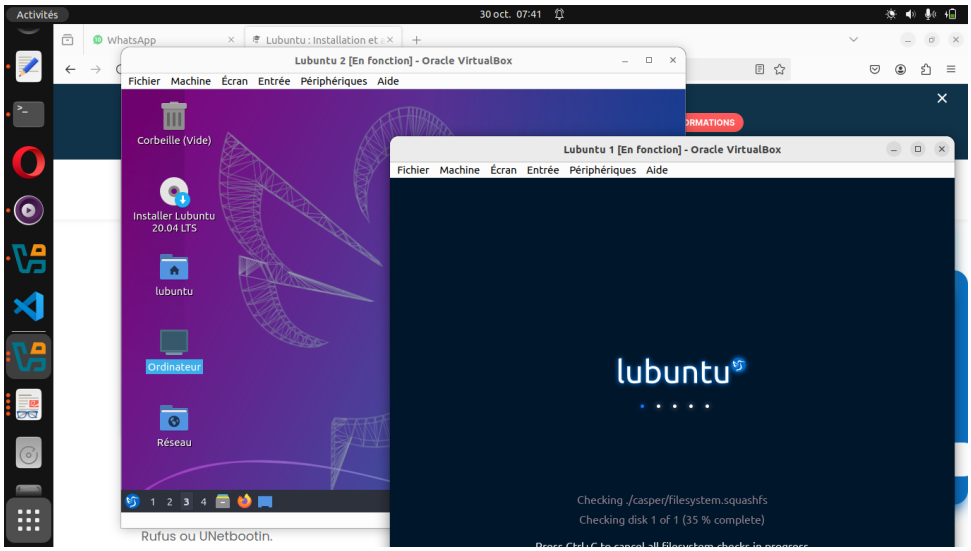


Figure 2.7: Machine Lubuntu.

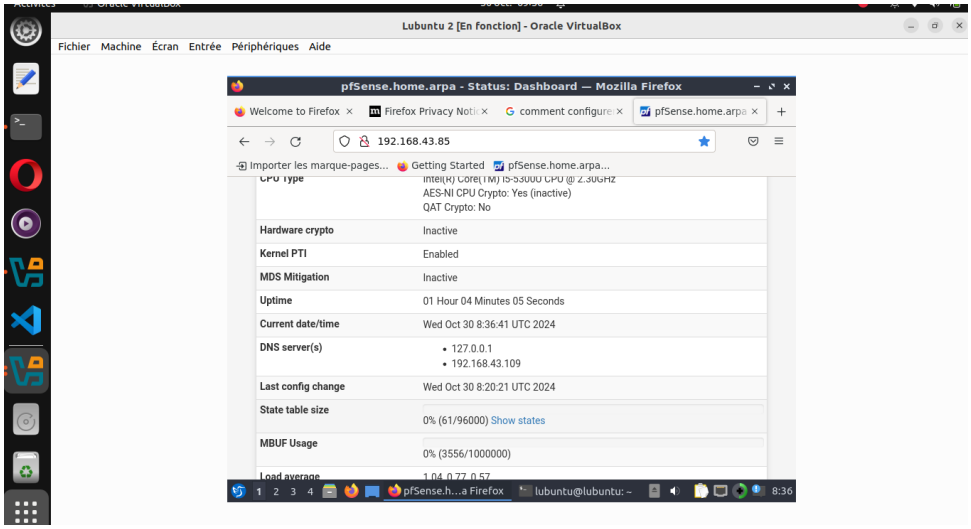


Figure 2.8: Interface pfSense.

2.6.5 Les différents onglets de pfSense

Nous avons des onglets qui fournissent plusieurs services :

- **System** : Permet de faire l'ensemble des réglages concernant le système en lui-même.
- **Interfaces** : Permet la gestion des interfaces réseau (`LAN` et `WAN`).
- **Firewall** : Permet de mettre en place toutes les règles servant de pare-feu.
- **Services** : Permet d'activer de nombreux services faisant de pfSense un firewall multifonction pouvant se transformer en serveur/relais DHCP ou bien encore en portail captif.
- **VPN** : Permet d'activer/désactiver le `VPN` et de mettre en place une sécurité via `IPSec`.
- **Status** : Permet de voir le statut de l'ensemble des configurations.
- **Diagnostics** : Permet de donner des outils permettant le diagnostic d'un quelconque bug.

2.6.6 Activation des protocoles de sécurité de pfSense

Pour éviter les intrusions au réseau local `LAN`, nous devons effectuer quelques configurations :

- Activer le **HTTPS** pour que la connexion entre l'ordinateur et le serveur soit chiffrée ;
- Changer le numéro du port pour accéder à l'interface web ;
- Cocher la case pour supprimer la redirection automatique vers l'interface web lors de la connexion à l'adresse IP du serveur sur le port 80 ;

- Activer le **SSH** pour éviter de passer par la console ;
- Cocher la case si vous désirez que le mot de passe de l'interface web soit demandé lors de l'accès à la console.

Pour activer les protocoles **HTTPS** et **SSH**, nous procédons comme suit :

1. Aller dans l'onglet `System` de pfSense ;
2. Cliquer sur **System** → **Advanced** → **Admin Access**.

Chapter 3

Architecture et Supervision

3.1 Architecture fonctionnelle

3.1.1 Description du fonctionnement

pfSense agit comme un point de contrôle entre différents segments réseau, gérant le trafic entrant et sortant. En tant que pare-feu et routeur, il filtre les paquets de données et décide lesquels autoriser ou bloquer en fonction des règles prédéfinies.

3.1.2 Collecte de données via SNMP ou NetFlow

pfSense peut collecter des données réseau via des protocoles comme SNMP (Simple Network Management Protocol) ou NetFlow. Ces protocoles permettent la surveillance du trafic réseau, aidant à identifier les anomalies et à optimiser les performances.

3.1.3 Interfaces web pour administrateurs et utilisateurs techniques

pfSense offre des interfaces web intuitives et accessibles pour les administrateurs et les utilisateurs techniques, facilitant la gestion et la configuration des réseaux.

3.2 Gestion des alertes et notifications

3.2.1 Configurations pour les alertes par email ou SMS

pfSense permet de configurer des alertes par email ou SMS pour notifier les administrateurs en cas d'événements critiques, tels que les tentatives d'intrusion ou les anomalies de performance.

3.2.2 Notifications personnalisables selon les règles

Les notifications peuvent être personnalisées selon des règles prédéfinies, offrant une flexibilité et une réactivité accrues en fonction des besoins spécifiques du réseau.

3.3 Architecture de déploiement

3.3.1 Composants utilisés (matériel et technologies)

La mise en œuvre de pfSense implique plusieurs composants, notamment :

- **Matériel** : Un serveur ou une machine avec au moins deux cartes réseau.
- **Technologies** : Utilisation de FreeBSD, Squid pour le proxy, et Snort pour la détection d'intrusions.

3.3.2 Schéma de déploiement avec diagramme des zones réseau

Le déploiement de pfSense peut être visualisé avec un schéma montrant les zones réseau protégées, incluant les segments WAN (Wide Area Network), LAN (Local Area Network), et DMZ (Demilitarized Zone).

3.3.3 Exemples:

Architecture 1

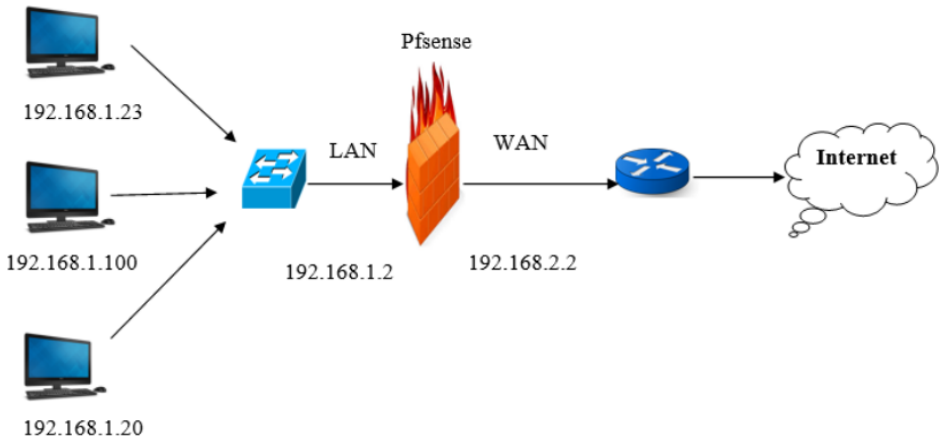


Figure 3.1: Réseau supervisé avec Pfsense 1

Architecture 2

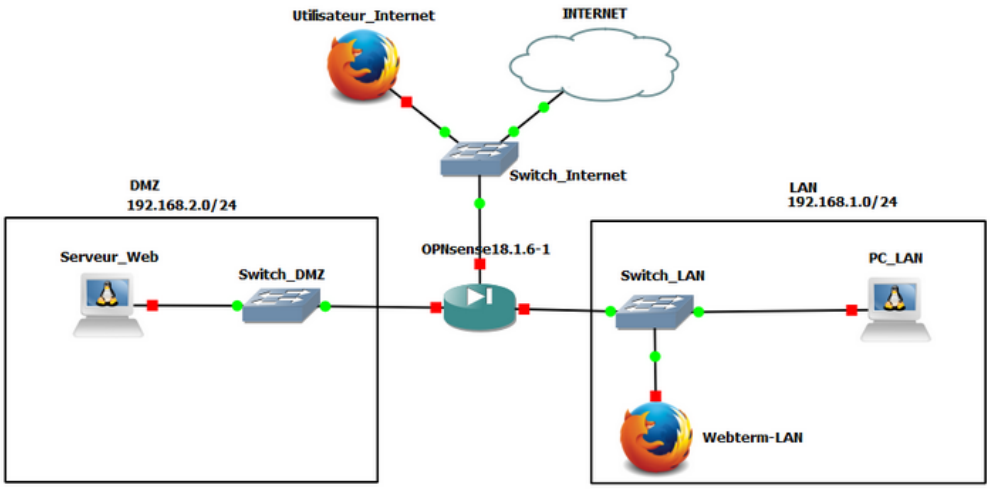


Figure 3.2: Réseau supervisé avec Pfsense 2

3.4 Configurations attendues

3.4.1 Exigences matérielles et paramétrage réseau

Les exigences matérielles pour pfSense incluent :

- **RAM** : 2 Go ou plus
- **CPU** : Multicœur

Le paramétrage réseau peut inclure des adresses IP statiques et des règles de NAT (Network Address Translation).

3.4.2 Modules et plugins (Squid, Snort)

- **Squid** : Utilisé pour le caching proxy, améliorant les performances en stockant les contenus fréquemment demandés.
- **Snort** : Un système de détection d'intrusion (IDS) pour identifier et prévenir les attaques.

3.4.3 Commandes et procédures pour l'installation

Les commandes et procédures d'installation de ces modules peuvent être effectuées via l'interface web ou le terminal FreeBSD.

3.5 Supervision et gestion des journaux

3.5.1 Suivi des métriques (CPU, mémoire, trafic réseau)

pfSense offre des outils pour suivre les métriques en temps réel telles que l'utilisation du CPU, de la mémoire, et le trafic réseau, aidant ainsi à maintenir des performances optimales.

3.5.2 Analyse des journaux pour identifier les problèmes

Les journaux de pfSense peuvent être analysés pour identifier les problèmes de sécurité ou de performance, fournissant des informations essentielles pour le dépannage.

3.6 Procédures de sauvegarde et de restauration

3.6.1 Sauvegarde manuelle et automatisée

pfSense permet des sauvegardes de configuration manuelles ou automatisées, garantissant que les paramètres réseau peuvent être restaurés en cas de besoin.

3.6.2 Restauration de la configuration

Les configurations sauvegardées peuvent être facilement restaurées via l'interface web de pfSense, minimisant le temps d'arrêt en cas de problème.

3.7 Limites de pfSense

Bien que pfSense soit puissant et flexible, il peut ne pas convenir aux infrastructures extrêmement complexes sans l'ajout de plugins ou de compétences avancées en administration réseau.

Chapter 4

Tests Réseau avec pfSense et Scénario

Pour la bonne administration de notre réseau, nous avons réalisé différents tests notamment :

- Création d'un portail Captif,
- Configuration d'un Traffic Shaper,
- Stress Testing.

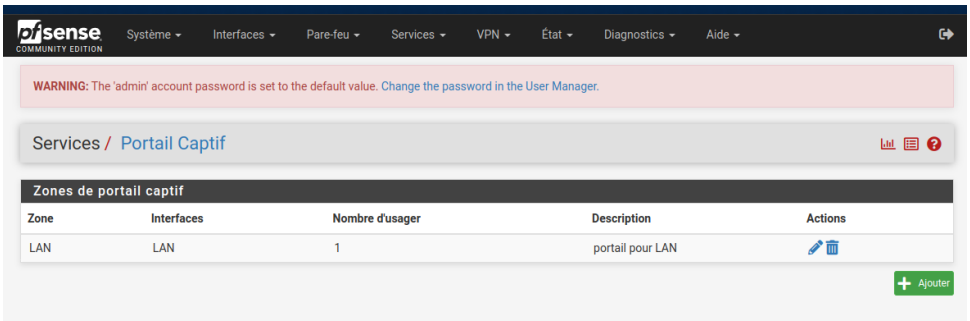
4.1 Création d'un portail captif

Un portail captif est une page web qui s'affiche automatiquement lorsqu'un utilisateur se connecte à un réseau Wi-Fi ou à un réseau informatique (le réseau LAN dans notre cas). Il permet d'autoriser seulement les utilisateurs qui ont accès au réseau à se connecter à partir d'un *username* et d'un *password*.

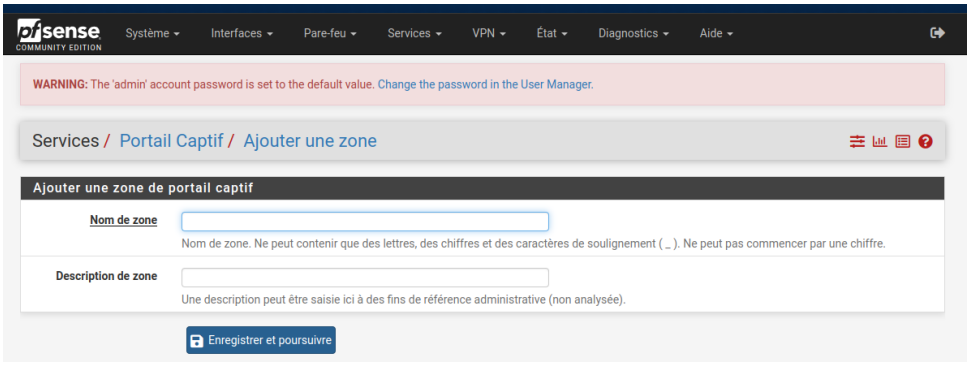
Étapes de configuration

NB : On considère que le réseau est déjà bien installé et configuré.

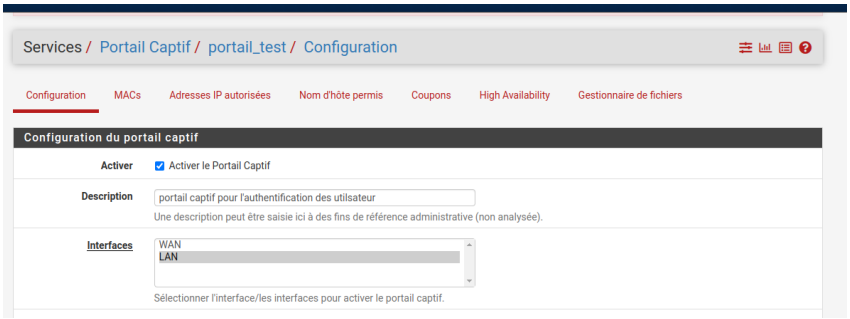
1. Aller dans la section **Services** → **Portail Captif** et cliquer sur *Ajouter*.

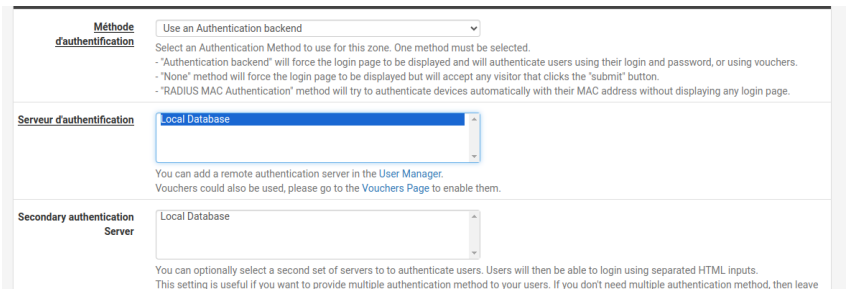


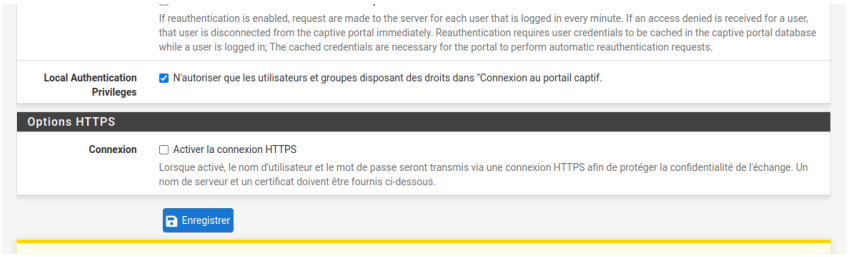
2. Ajouter le nom d'une zone et une description.



3. **Configurer le portail captif :**
   - Activer le portail captif,
   - Choisir l'interface (LAN ou MAN),
   - Choisir le mode d'authentification :
     - **Authentication Backend :** les utilisateurs s'authentifient avec un *username* et un *password*,
     - **None :** la page de connexion s'affiche, mais tout utilisateur qui clique sur *submit* aura accès au réseau,
     - **RADIUS MAC Authentication :** authentification basée sur les adresses MAC des utilisateurs, sans passer par la page de connexion.
4. Puis **Enregistrer**.



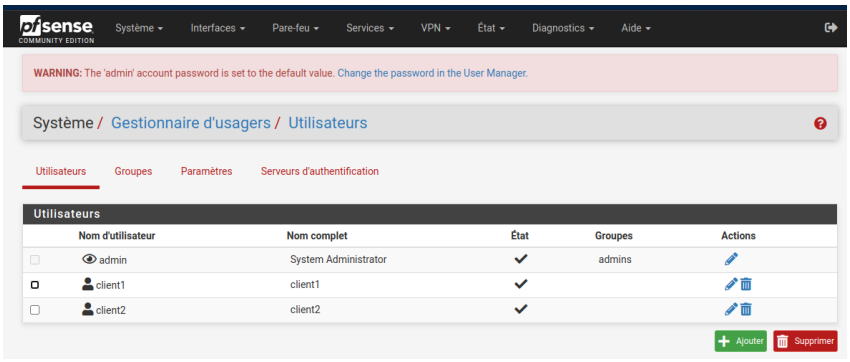




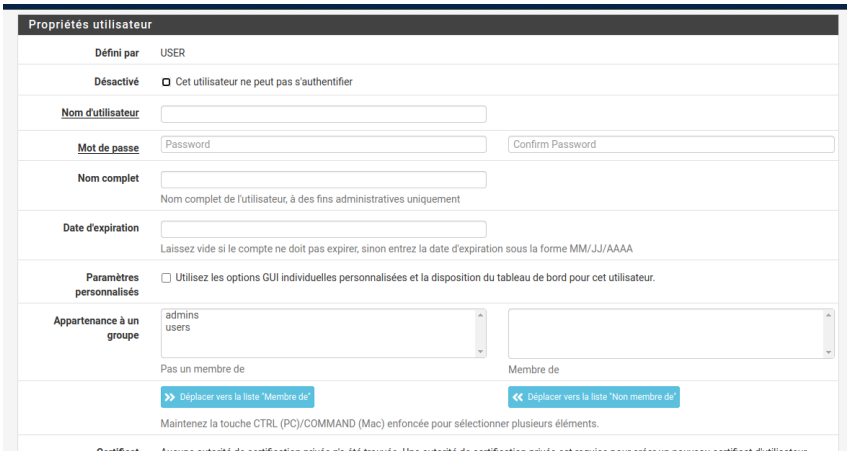
NB : On peut ajouter d'autres options et/ou personnaliser la page de connexion. Le portail captif est ainsi prêt.

Création d'un utilisateur

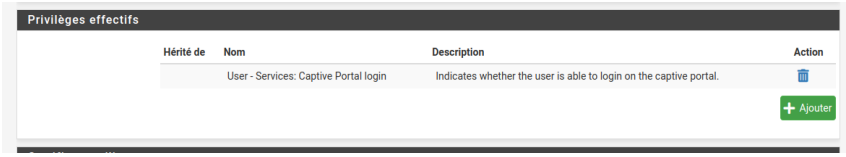
1. Aller dans **Système → Gestionnaire d'utilisateurs**.



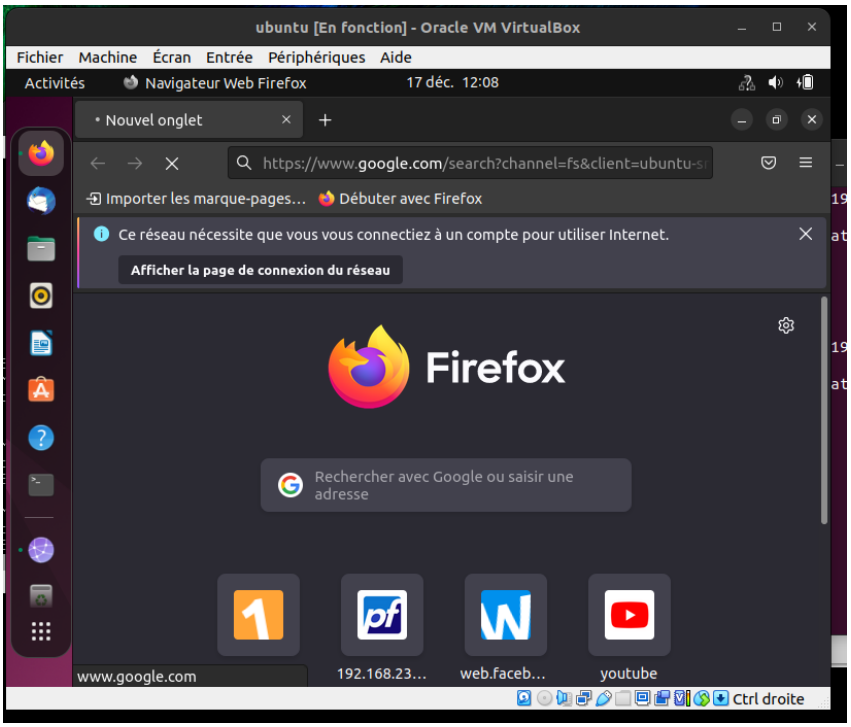
2. Cliquer sur *Ajouter*.
3. Définir les informations de l'utilisateur : nom, mot de passe, date d'expiration (si nécessaire) et les groupes d'accès.
4. Enregistrer.

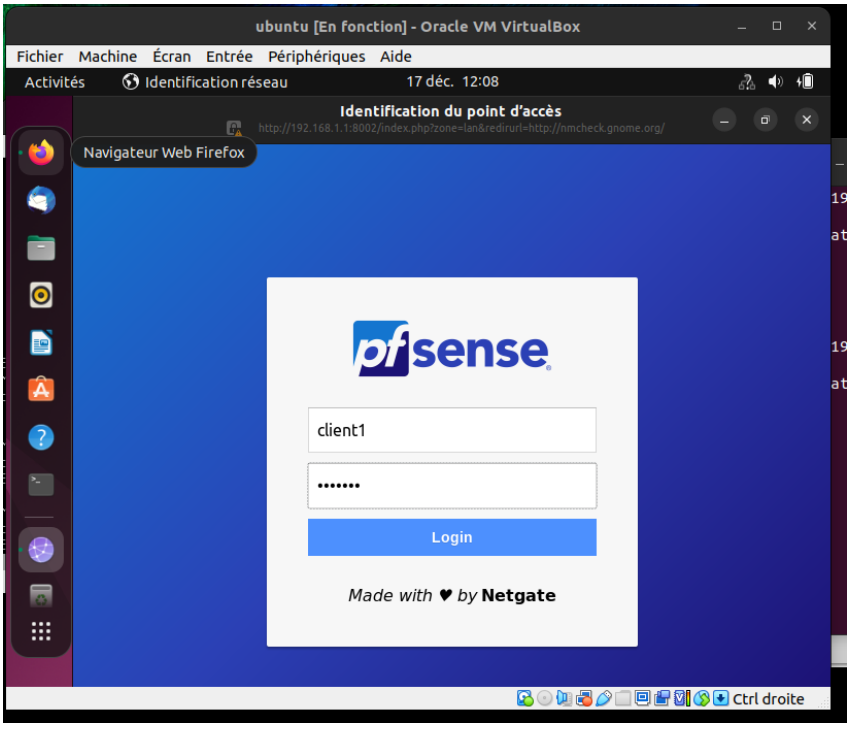


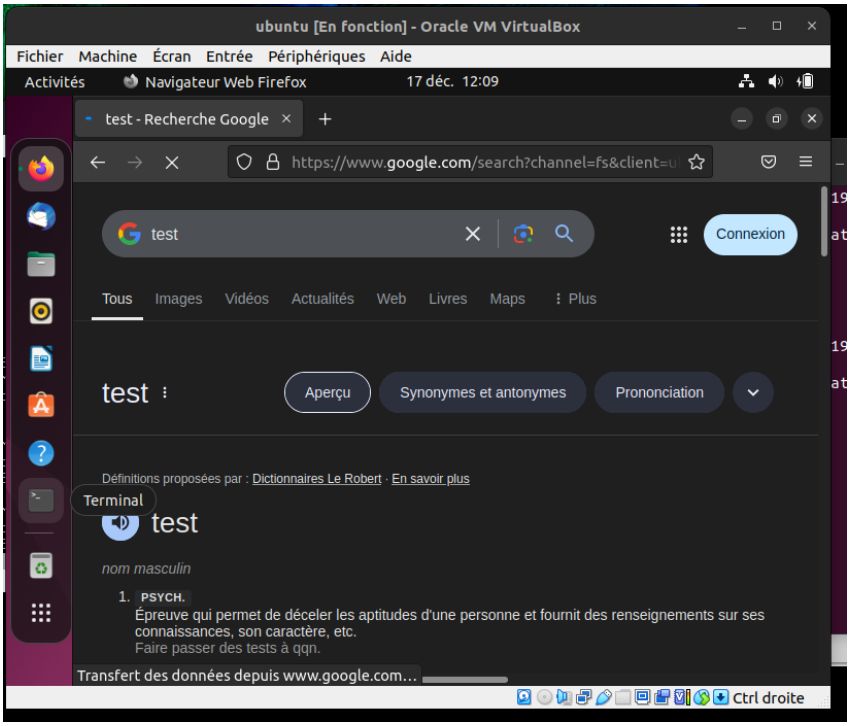
5. Définir les privilèges de l'utilisateur et valider.

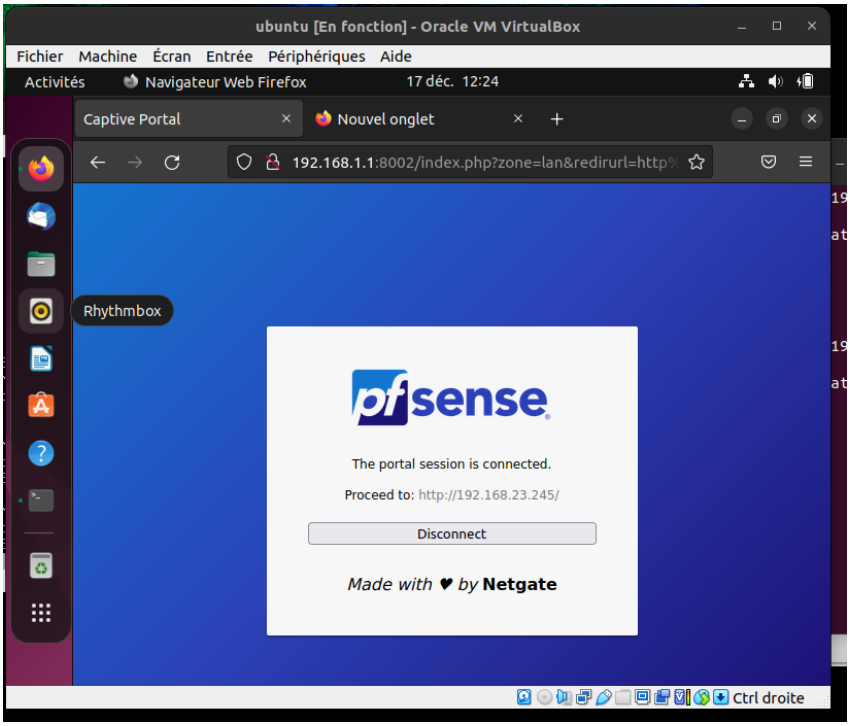

Privilèges effectifs
Hérité de
Nom
Description
Action
User - Services: Captive Portal login
Indicates whether the user is able to login on the captive portal.
Ajouter

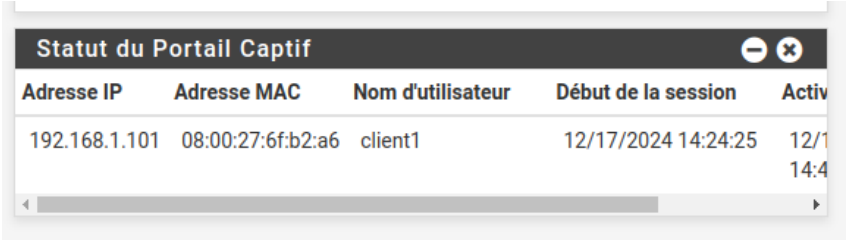
6. Tester


ubuntu [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités
Navigateur Web Firefox
17 déc. 12:08
• Nouvel onglet
https://www.google.com/search?channel=fs&client=ubuntu-s
Importer les marque-pages...
Débuter avec Firefox
Ce réseau nécessite que vous vous connectiez à un compte pour utiliser Internet.
Afficher la page de connexion du réseau
Firefox
Rechercher avec Google ou saisir une adresse
www.google.com
192.168.23...
web.faceb...
youtube
Ctrl droite


ubuntu [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités
Identification réseau
17 déc. 12:08
Identification du point d'accès
Navigateur Web Firefox
pfsense
client1
Login
Made with ♥ by Netgate
Ctrl droite







Le statut du portail captif affiche les différents utilisateurs connectés via celui-ci.

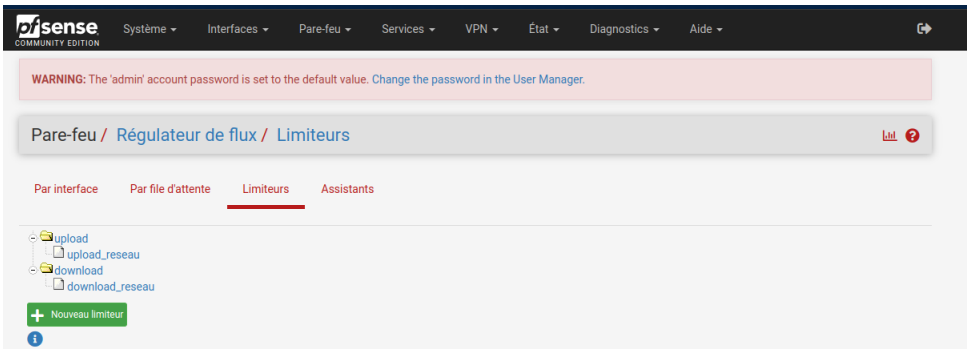
4.2 Configuration du Traffic Shaper

Le *Traffic Shaper* est une technique utilisée pour contrôler et gérer le trafic réseau, en particulier pour les réseaux à large bande. Il permet de limiter la bande passante consommée par certaines applications ou utilisateurs. Les techniques incluent :

- La limitation de débit,
- La mise en file d'attente,
- La priorisation du trafic.

Étapes de configuration

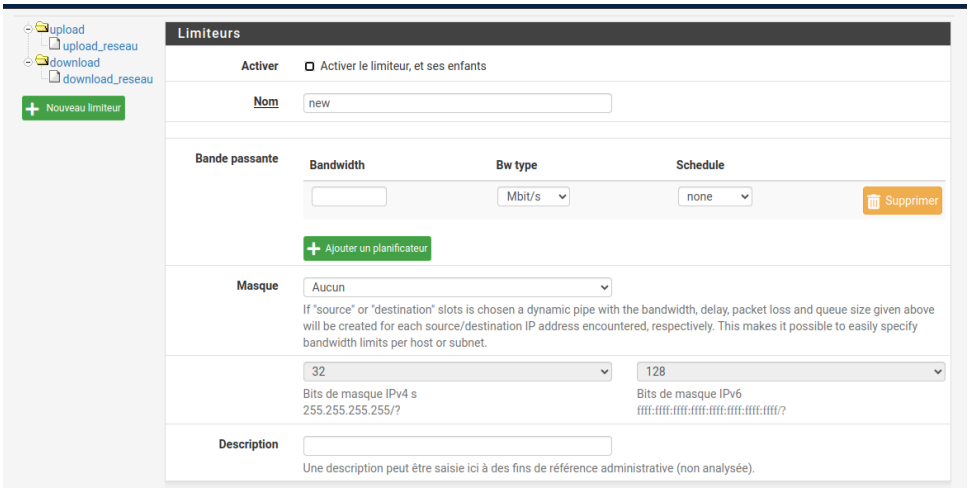
1. Aller dans **Pare-feu → Régulateur de flux → Limiteurs**.



4.2.1 Cliquer pour Créer un nouveau limiteur

.

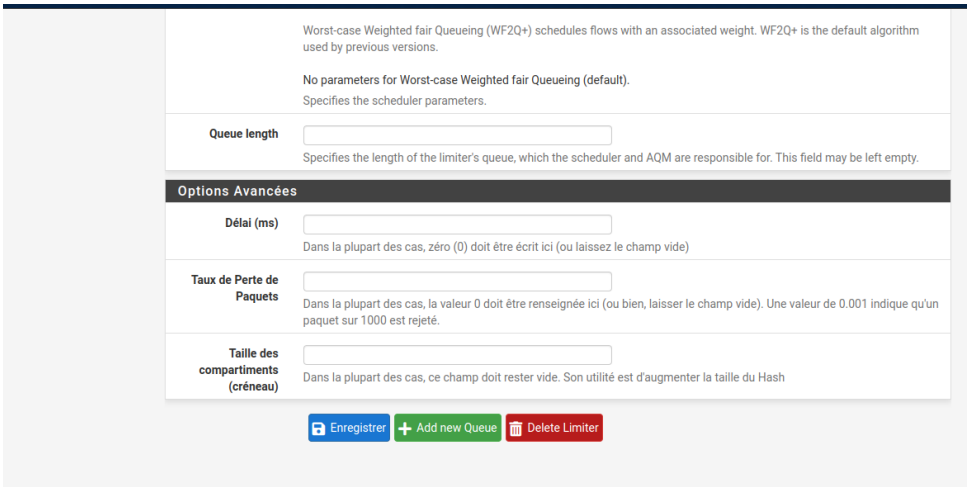
2. **Création du limiteur pour le trafic entrant :**



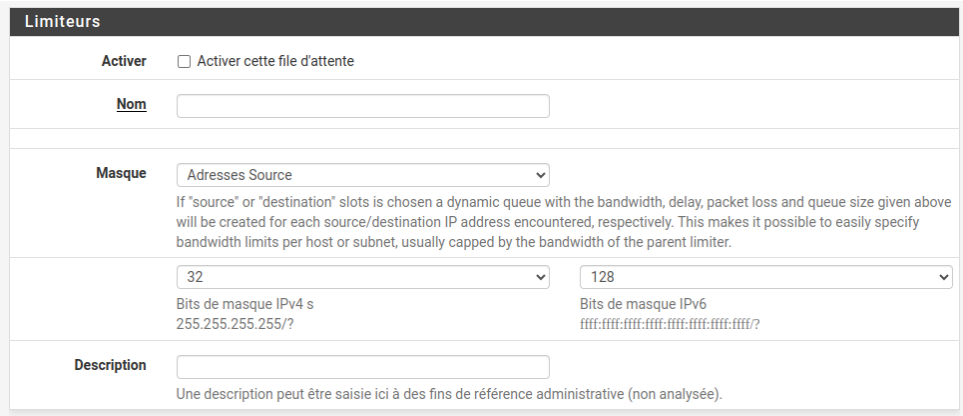
- Activer le limiteur,
- Donner un nom,
- Définir la bande passante et l'unité,

- Definir le type d'adresse (adresse source, adresse destination),
- Donner un destination et enregistrer.

4.2.2 Definr un nouvelle file d'attente :



- Activer la file d'attente,
- Donner un nom différent à celui du délimiteur,
- Préciser l'adresse source, le masque et une description si besoin.

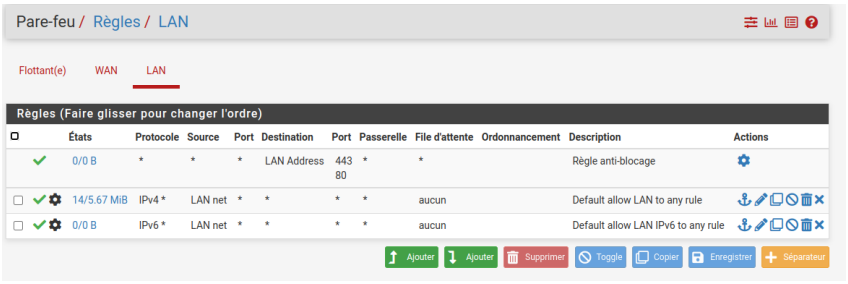


- Enregistrer.

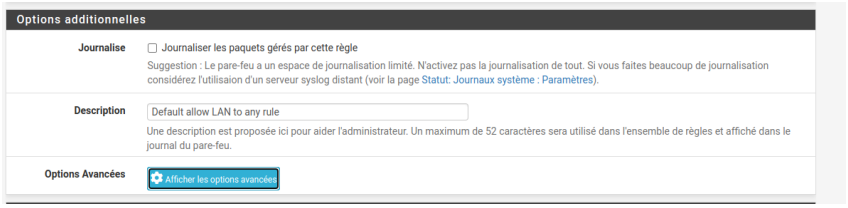
3. **création du limiteur pour le trafic sortant:**
4. Le processus est le même mais faut bien différencier les noms

4.2.3 Ajouter les limiteurs aux règles du pare-feu :

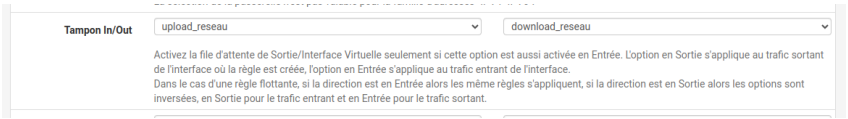
- Aller dans **Pare-feu → Règles → LAN**

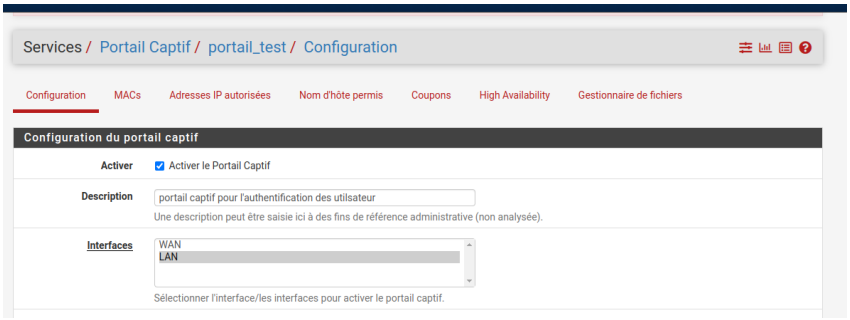


- Cliquer sur le crayon pour modifier les paramètres avancés,



- Modifier le *Tampon In/Out* pour ajouter les limiteurs créés.





Résultats des tests

Nous avons configuré le limiteur pour que le débit ne dépasse pas 20Kbps.

Avant l'activation des limiteurs :

Après l'activation des limiteurs :

4.3 Stress Testing

Le *Stress Testing* est une technique permettant d'évaluer les capacités d'un système à résister à des charges extrêmes et des scénarios de défaillance. Son objectif est de simuler des conditions de fonctionnement critiques telles que:

- Une charge utilisateur élevée,
- des Volumes de données importants,
- des Temps de réponse critiques,
- des Pannes ou défaillances du système.

Pratique

Avant le stress testing

Date/Heure actuels	Tue Dec 17 15:41:17 UTC 2024
Serveur(s) DNS	• 127.0.0.1 • 192.168.43.1
Dernière modification de la configuration	Tue Dec 17 15:11:07 UTC 2024
Taille de la table d'état	0% (33/96000) Afficher les états
Utilisation MBUF	0% (3556/1000000)
Moyenne de charge	0.18, 0.26, 0.25
Utilisation CPU	11%
Utilisation de la mémoire	28% of 961 MiB
Utilisation de la mémoire d'échange (SWAP)	0% of 1024 MiB

Commande utilisée pour le stress testing :
Exemple: `sudo hping3 -S -p 80 -flood 245`
Execution

```
xponentiel@xponentiel-Latitude-E5440:~$ sudo hping3 -S -p 80 --flood 192.168.23.
245
[sudo] Mot de passe de xponentiel :
HPING 192.168.23.245 (wlp2s0 192.168.23.245): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

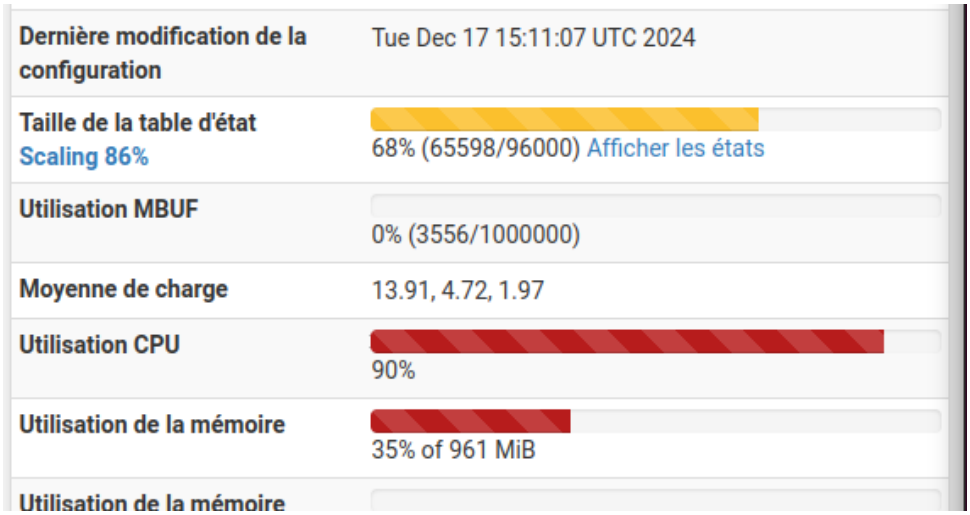
Explication:

- **-S** : Précise les informations de source et de port,
- **-p 80** : Spécifie le port cible (ici, le port 80),
- –**flood** : Envoie des paquets en continu sans attendre de réponse,
- **245** : Définit le nombre ou la taille des paquets à envoyer.

Autre Exemple:

```
xponentiel@xponentiel-Latitude-E5440:~$ sudo hping3 -S -p 80 --flood 192.168.43.
190
HPING 192.168.43.190 (wlp2s0 192.168.43.190): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.43.190 hping statistic ---
4421730 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
xponentiel@xponentiel-Latitude-E5440:~$
```

La consommation CPU a fortement augmenté durant le test.


Dernière modification de la configuration
Tue Dec 17 15:11:07 UTC 2024
Taille de la table d'état
Scaling 86%
68% (65598/96000) Afficher les états
Utilisation MBUF
0% (3556/1000000)
Moyenne de charge
13.91, 4.72, 1.97
Utilisation CPU
90%
Utilisation de la mémoire
35% of 961 MiB
Utilisation de la mémoire

Conclusion

pfSense est un outil de supervision réseau puissant et polyvalent, offrant une gamme complète de fonctionnalités de sécurité et de gestion. Sa base sur FreeBSD lui assure stabilité et performances, tandis que ses options de configuration et d'intégration en font une solution adaptée à divers environnements réseau.

Grâce aux différentes configurations et tests réalisés, notamment le portail captif, le traffic shaper et le stress testing, nous avons pu évaluer, optimiser et renforcer les performances du réseau. Ces étapes ont permis de garantir un usage fiable, sécurisé et maîtrisé de l'infrastructure réseau, répondant ainsi aux exigences de robustesse et de performance attendues dans un environnement de production.

Annexes

Références

Voici quelques ressources supplémentaires pour approfondir l'utilisation de pfSense et la gestion de la sécurité réseau :

- pfSense - Site officiel : Ressource principale pour télécharger pfSense, consulter des guides, forums et plus.
- Malekal - Sécurité informatique avec pfsense : Site spécialisé en sécurité informatique avec des tutoriels et des conseils pour la protection de votre réseau.
- Cours sur pfsense Classroom
- AI d'aide
- Google
- Ecriture des rapports en latex en ligne gratuit
- Assist: Salvador Delibes