

MANOLIOS Benjamin

EPSI Montpellier

N° candidat : 02443855566

Épreuve E6

Situation N°1

Mise en place d'un pare-feu pfSense pour sécuriser le réseau d'entreprise

BTS SIO SISR 2024/2025

Benjamin MANOLIOS

Sommaires :

Sommaires :	2
Contexte	3
<i>CLIENT</i> :	3
Description :	4
Problème :	4
Solution :	Erreur ! Signet non défini.
Réseaux avant modification :	5
On y retrouve :	5
Solution :	6
Problème :	6
Solution :	6
Avantages :	7
Inconvénients :	7
Réseaux après modification.....	7
Installation Pfsense	8
Interface console de pfSense	12
II.Configuration de pfSense	13
Configuration web	13
Conclusion.....	15

Contexte

Je suis actuellement employé à la Maison des Ligues de Lorraine (M2L), un établissement dépendant du Conseil Régional de Lorraine. Elle a pour mission de soutenir les ligues sportives régionales en leur fournissant des services logistiques, administratifs et techniques. La M2L héberge plusieurs structures dans différents bâtiments, proposant des bureaux équipés, des salles mutualisées (réunion, formation, amphithéâtre) et un accès à un réseau informatique commun.

Le réseau de la M2L dessert un grand nombre d'utilisateurs répartis dans plusieurs bâtiments. Certains sont récents et équipés en gigabit Ethernet, d'autres plus anciens, avec des équipements hétérogènes. Le réseau actuel manque de centralisation et de sécurité : la distribution d'adresses IP, le filtrage, et la segmentation ne sont pas uniformisés.

Pour moderniser son infrastructure et renforcer la sécurité, la M2L souhaite mettre en place un routeur virtuel basé sur **pfSense**, un logiciel libre qui permet de gérer le réseau et d'assurer la sécurité (comme un pare-feu professionnel).

Ce routeur sera capable de gérer :

- **Le routage et la distribution IP via DHCP**, un service qui attribue automatiquement une adresse IP à chaque appareil connecté,
- **Le filtrage réseau grâce à un pare-feu**, un système qui contrôle les connexions autorisées ou bloquées pour protéger le réseau,
- **La gestion des VLANs**, qui permettent de séparer logiquement les utilisateurs sur le même réseau pour plus de sécurité et de clarté.

La solution est déployée sur une infrastructure virtualisée avec **Proxmox VE**, un outil qui permet de créer et gérer plusieurs machines virtuelles (VM) sur un seul serveur physique. Le serveur utilisé est un ASUS PRO Q570M, hébergeant pfSense et plusieurs machines clientes (Windows/Linux).

Ce projet permet à la M2L de mieux sécuriser ses services, et me permet de mettre en œuvre des compétences clés du BTS SIO SISR, notamment en **administration réseau**, **virtualisation** et **sécurité informatique**.

CLIENT :

Maison des Ligues de Lorraine (M2L)

Description :

La Maison des Ligues de Lorraine (M2L) est un établissement public placé sous la responsabilité du Conseil Régional de Lorraine. Elle a pour mission de soutenir les différentes **ligues sportives régionales** en leur fournissant des locaux, des services logistiques, des équipements informatiques, ainsi qu'un accès à une infrastructure réseau partagée.

Avec l'augmentation du nombre de structures hébergées, la M2L doit renforcer la sécurité et la gestion de son réseau interne. C'est dans ce cadre que le projet de mise en place d'un **routeur virtuel pfSense** a été initié. L'objectif est d'assurer une **distribution efficace des services réseau**, tout en garantissant une **bonne séparation des flux** (LAN / DMZ / VLAN), et une **protection renforcée via un pare-feu**.

Redondance et sécurité du réseau avec pfSense

Problème :

Le réseau actuel, bien que fonctionnel, ne dispose pas de règles de sécurité avancées, ni d'un système centralisé pour gérer les accès, le routage et la distribution IP. Cela limite les possibilités de segmentation du réseau et expose l'infrastructure à des risques de mauvaise configuration ou d'attaques.

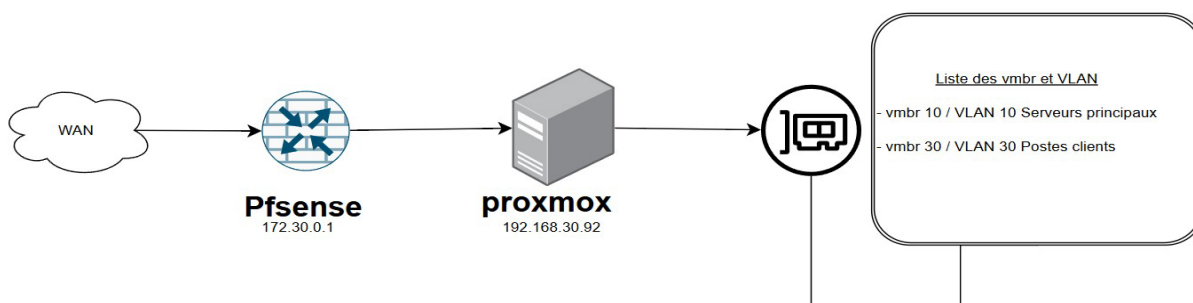
Solution :

Déployer un **pare-feu pfSense virtualisé** dans **Proxmox VE**, et le configurer comme **routeur principal** pour piloter le réseau de manière centralisée et sécurisée.

Les fonctionnalités mises en place incluent :

- **La gestion des interfaces LAN et DMZ** : le LAN correspond au réseau interne, tandis que la **DMZ** (zone démilitarisée) est une zone isolée qui héberge les services accessibles depuis l'extérieur (ex : un site web), sans exposer le réseau principal,
- **Le filtrage du trafic entrant et sortant** à l'aide de **règles précises**, créées dans pfSense pour contrôler les accès réseau selon leur origine, leur destination ou leur protocole,
- **La distribution des adresses IP via DHCP**, un service qui assigne automatiquement une adresse IP à chaque appareil connecté,
- **L'accès restreint aux bases de données depuis la DMZ**, pour éviter tout accès direct non autorisé aux données internes sensibles,
- **La configuration possible de VLAN**, qui permet de **séparer logiquement les services ou groupes d'utilisateurs** (ex : administration, invités, technique) sur le réseau pour plus de sécurité.

Réseaux avant modification :



Explication du schéma – VLAN et vmbr

- **VLAN (Virtual Local Area Network)** : permet de séparer logiquement le réseau en plusieurs zones pour mieux sécuriser et organiser les flux.
 - **VLAN 10** : serveurs principaux
 - **VLAN 30** : postes clients
- **vmbr (Virtual Machine Bridge)** : interface réseau utilisée dans Proxmox pour connecter les machines virtuelles à un VLAN spécifique.
 - **vmbr10** → **VLAN 10**
 - **vmbr30** → **VLAN 30**

Cette configuration isole les services et permet une meilleure gestion réseau avec pfSense.

Benjamin MANOLIOS

On y retrouve :

Un pare-feu pfSense

- Connecté à Internet (WAN)
- Adresse IP : 172.30.0.1
- Gère le routage, le DHCP et la sécurité du réseau

Un serveur Proxmox

- Adresse IP : 192.168.30.92
- Contient les machines virtuelles

Deux VLANs configurés :

- VLAN 10 : Serveurs principaux
- VLAN 30 : Postes clients

Malgré la présence de pfSense et de VLANs identifiés, aucune véritable segmentation réseau ni règles de sécurité spécifiques n'étaient mises en place, ce qui justifie la nécessité d'une refonte complète de l'architecture.

Solution :

Mise en place de pfSense pour sécuriser et structurer le réseau

Problème :

Le réseau de la M2L n'était pas segmenté et fonctionnait sans règles de sécurité avancées. Tous les équipements étaient connectés au même réseau, ce qui représentait un risque pour la sécurité. De plus, il n'existait aucun moyen de contrôler précisément les communications internes entre les postes, les serveurs et les services réseau.

Solution :

Pour répondre à ces besoins, j'ai mis en place pfSense, un pare-feu open source, en tant que routeur principal de l'infrastructure. Il a été installé sur une machine virtuelle via Proxmox. J'ai ensuite créé deux VLANs : un pour les serveurs (VLAN 10) et un pour les postes clients (VLAN 30). PfSense a été configuré pour gérer le routage entre ces VLANs, attribuer les adresses IP grâce au serveur DHCP intégré, et filtrer le trafic à l'aide de règles personnalisées. Cette configuration permet désormais de mieux organiser les flux réseau tout en renforçant la sécurité.

Benjamin MANOLIOS

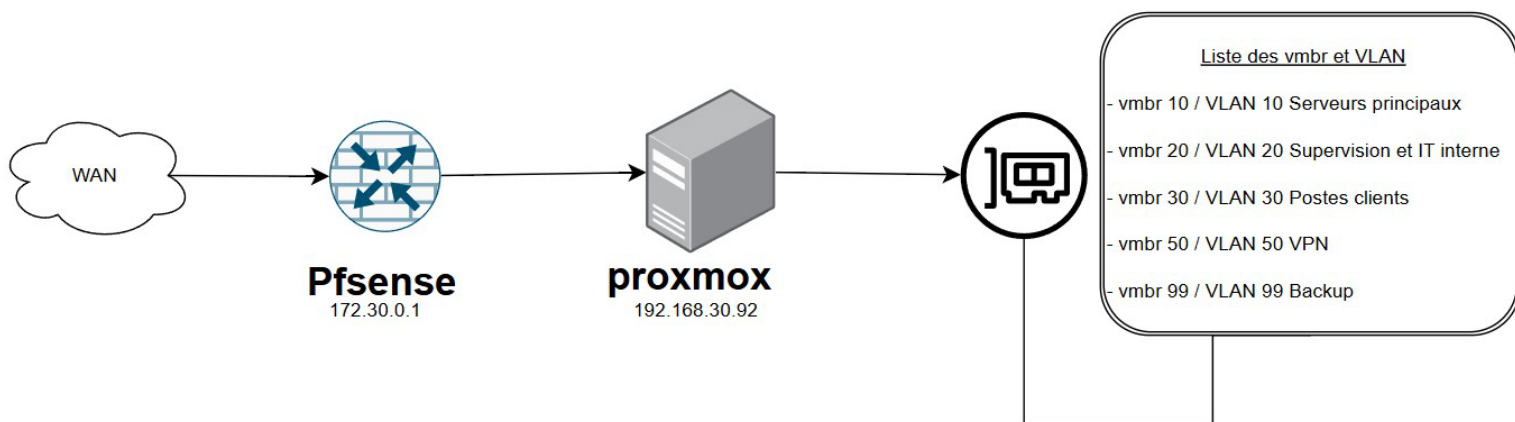
Avantages :

Cette solution permet d'améliorer considérablement la sécurité grâce à la séparation des machines par VLAN. Elle offre aussi une meilleure maîtrise du réseau, car les règles de filtrage peuvent être adaptées aux besoins de chaque zone. En plus d'être fiable, pfSense est une solution gratuite, ce qui en fait un choix économique pour l'organisation. L'administration du réseau est également facilitée grâce à une interface web claire et centralisée.

Inconvénients :

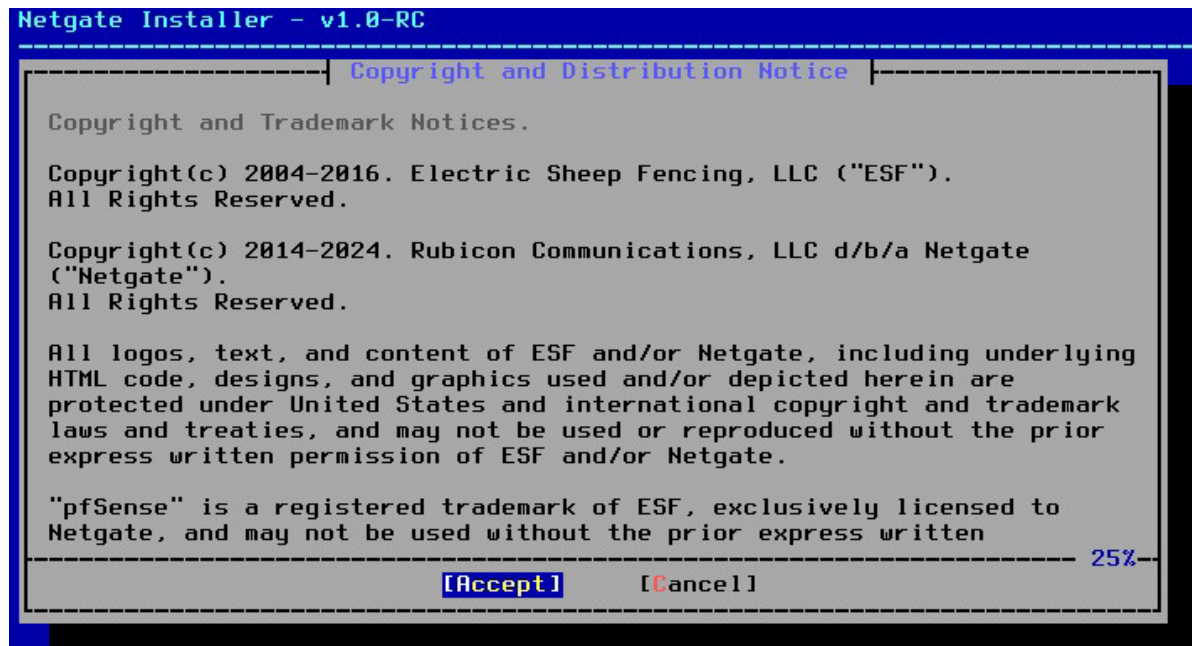
La configuration initiale de pfSense demande du temps et des connaissances techniques. Il faut définir manuellement les interfaces, les VLANs, les règles de parefeu, et s'assurer que tout fonctionne correctement. Une erreur de configuration peut impacter la connectivité. Toutefois, une fois correctement mis en place, pfSense reste stable, puissant et adapté aux besoins de la M2L.

Réseaux après modification :

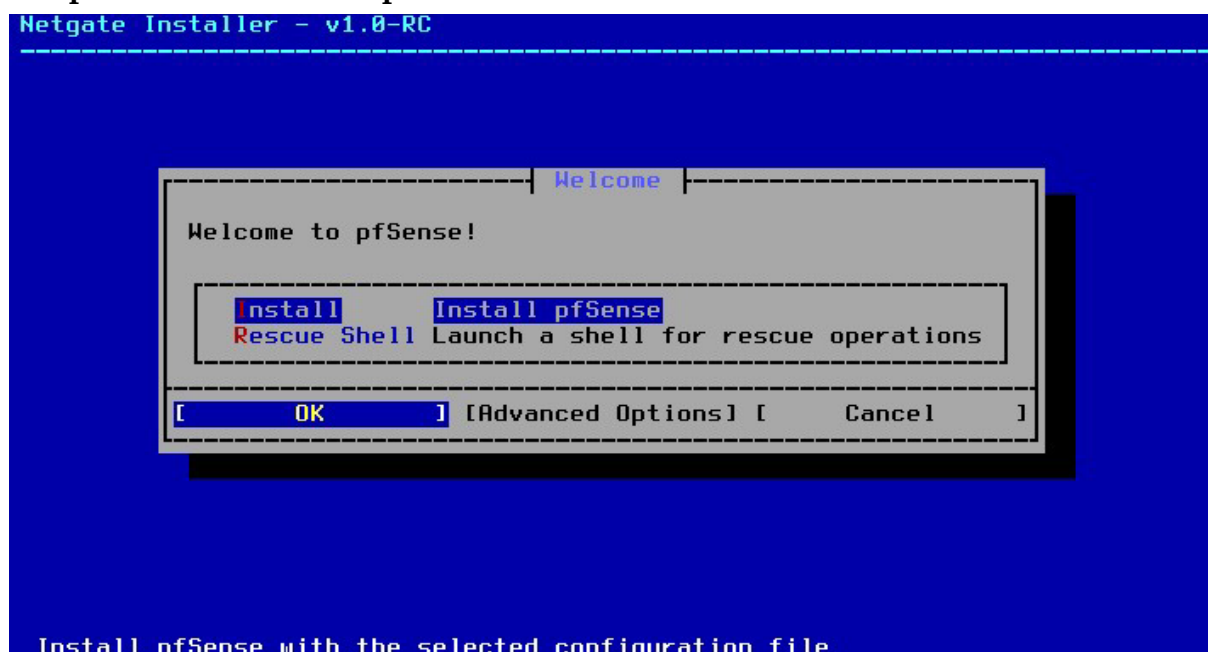


Installation Pfsense

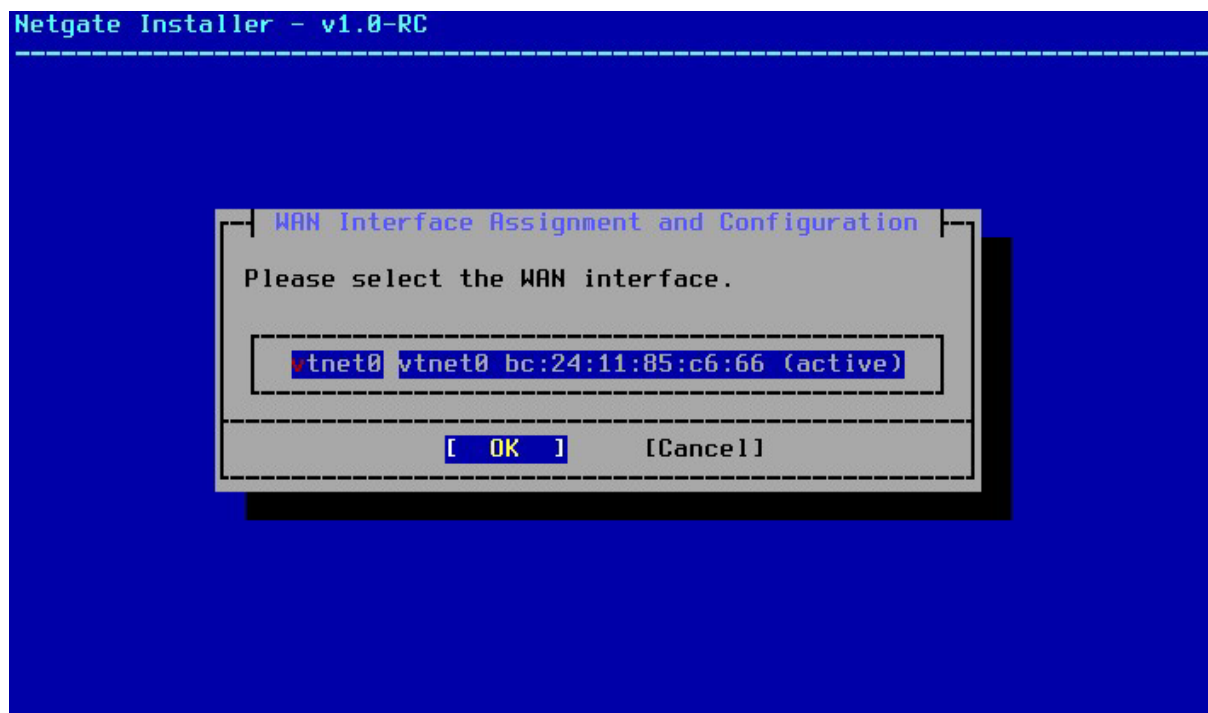
a- Pfsense installer



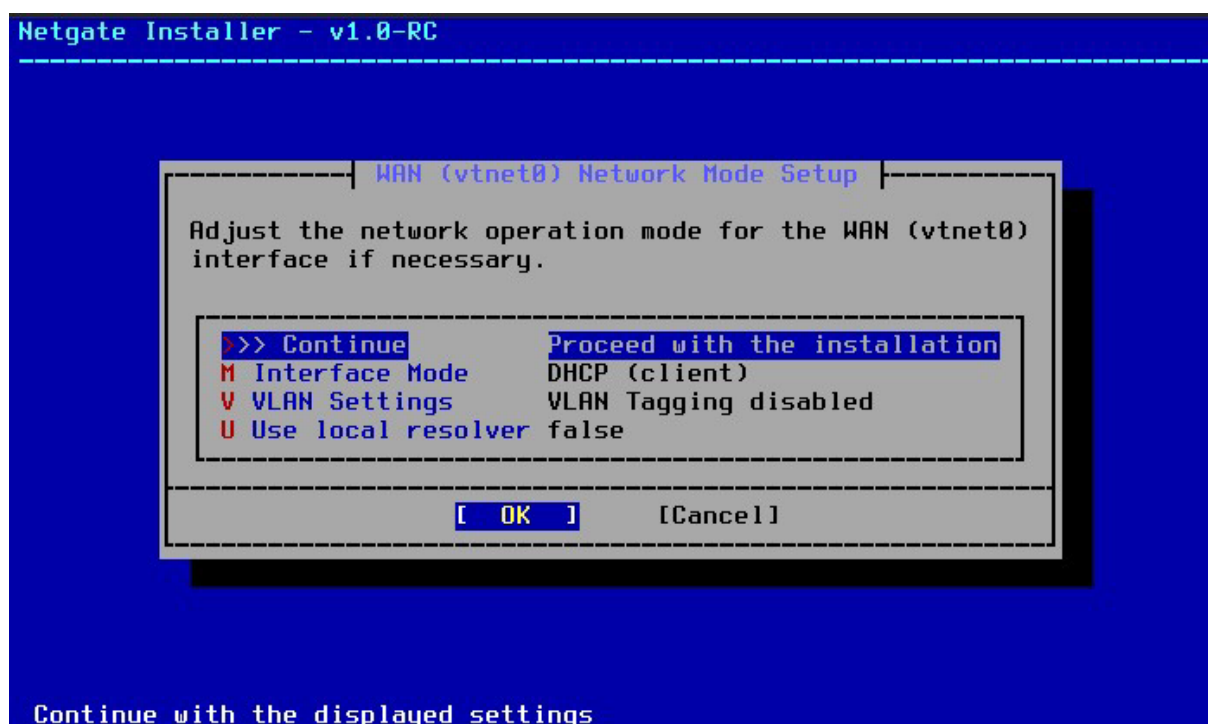
Sur l'écran de démarrage de l'installateur pfSense, il suffit d'appuyer sur Entrée pour accepter les conditions et poursuivre l'installation



Ici, l'installateur propose deux options principales : installer pfSense ou lancer un shell de secours. J'ai sélectionné "Install pfSense" puis validé en appuyant sur "OK".

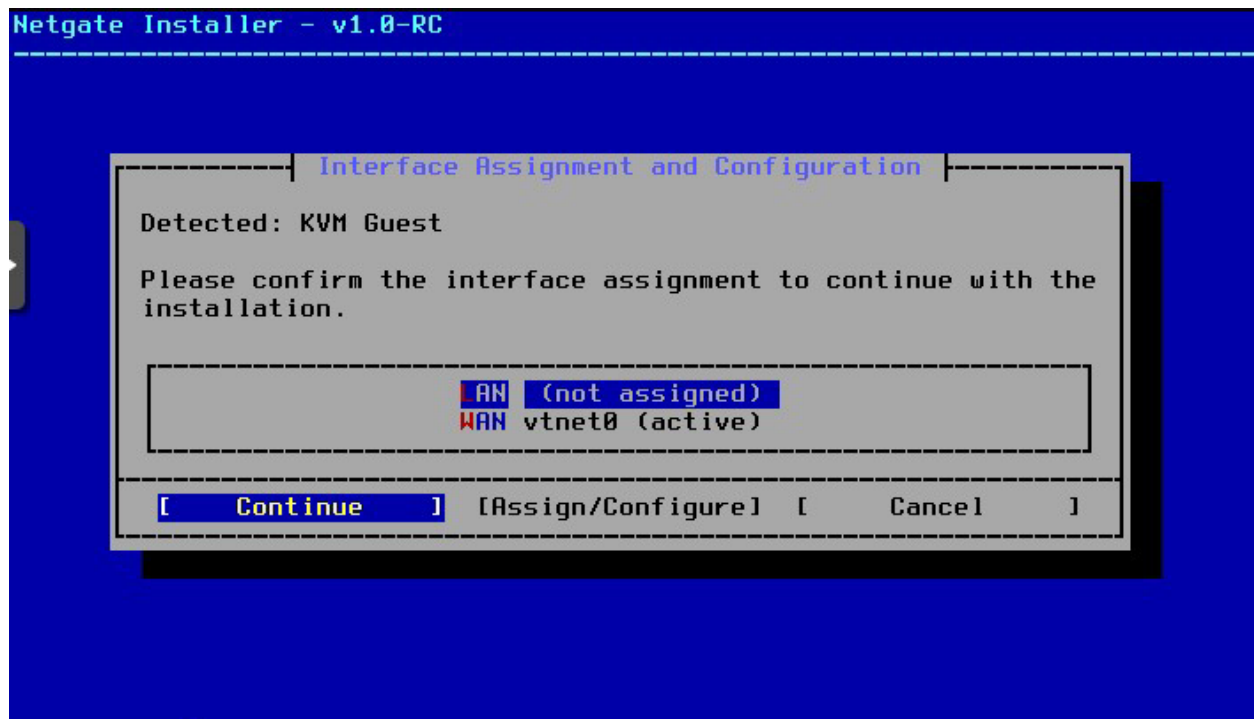


À cette étape, j'ai sélectionné l'interface réseau proposée pour la connexion WAN (ici "vtnet0") puis validé en appuyant sur "OK". Cela permet d'associer clairement l'interface WAN physique à pfSense.

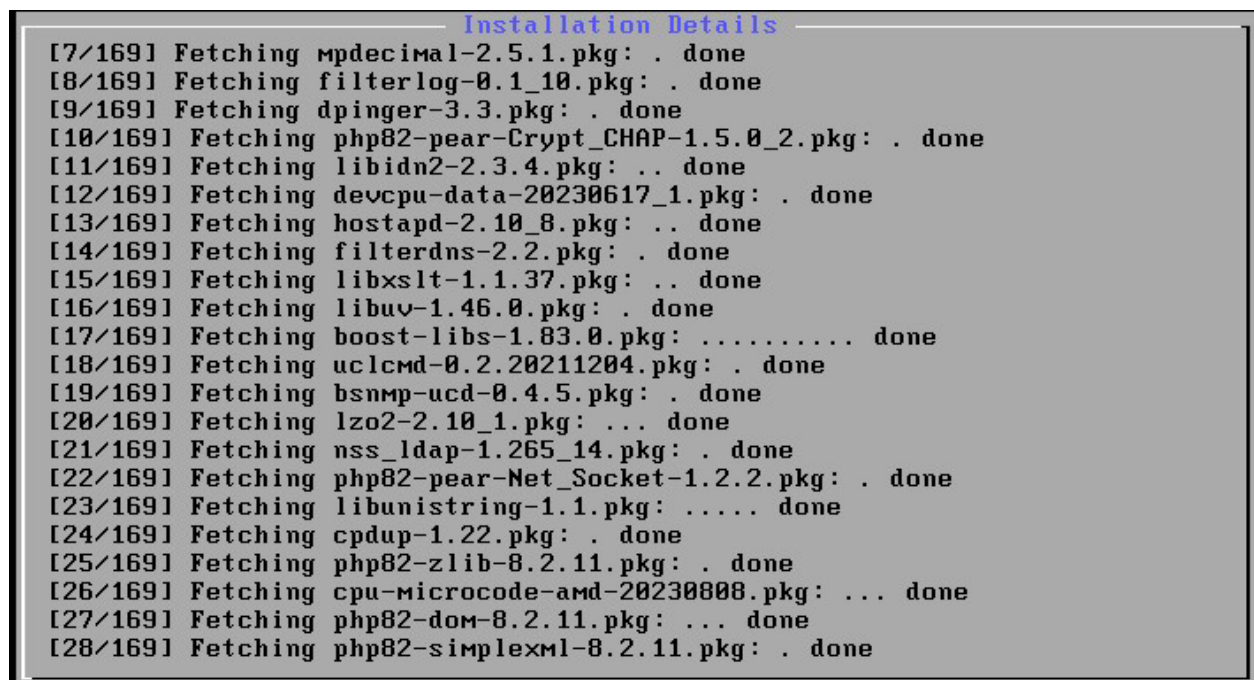


J'ai conservé les paramètres réseau par défaut proposés (DHCP pour WAN, VLAN désactivé, resolver local désactivé) en validant avec "Continue" puis "OK". Ces choix assurent une configuration initiale rapide avec une connectivité fonctionnelle immédiate.

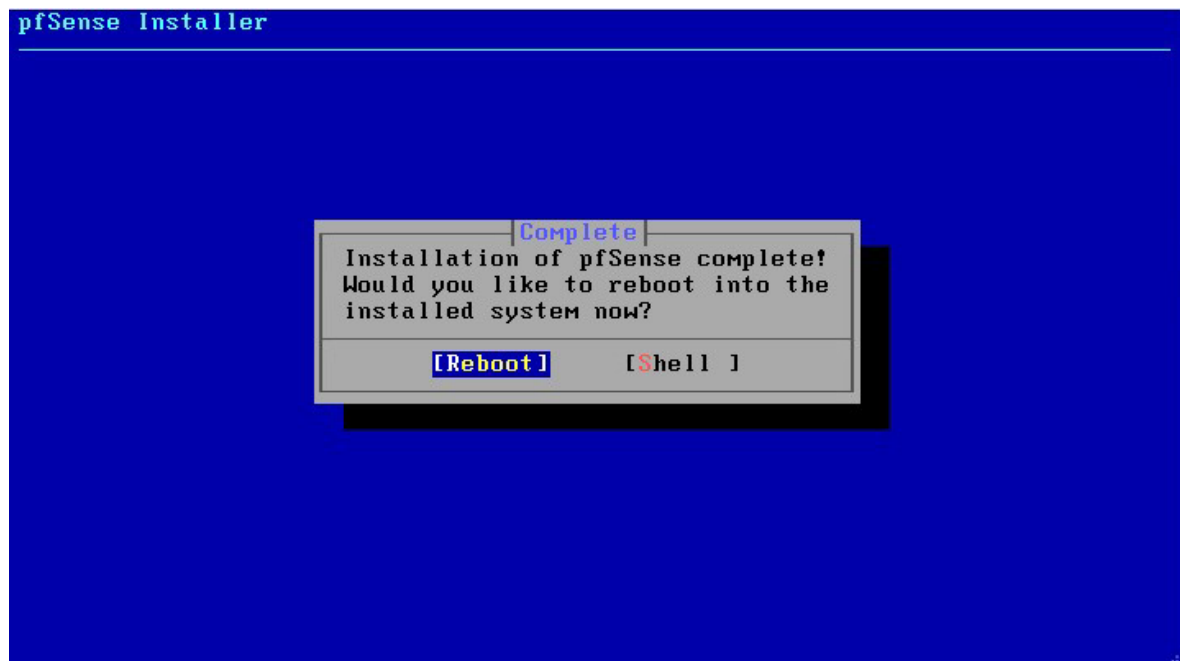
Benjamin MANOLIOS



À cette étape, pfSense détecte automatiquement les interfaces réseau disponibles. J'ai validé l'assignation proposée (WAN = vtnet0) en appuyant sur "Entrée" pour poursuivre.



Ici, l'installateur télécharge les paquets nécessaires au bon fonctionnement du système (libs, PHP, filtres, outils système, etc.). Ce processus est automatique et dure quelques minutes.



L'installation de pfSense est terminée. Un message invite à redémarrer la machine virtuelle. J'ai sélectionné "Reboot" pour lancer pfSense sur le disque dur installé.

```

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
KVM Guest - Netgate Device ID: 07699ea86a1416c0d95d

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.134/24
LAN (lan)      -> vtnet1      -> v4: 172.30.0.1/24
OPT1 (opt1)    -> vtnet2      -> v4: 10.10.10.1/32
OPT2 (opt2)    -> vtnet3      -> v4: 10.10.20.1/32
OPT3 (opt3)    -> vtnet4      -> v4: 10.10.30.1/32
OPT4 (opt4)    -> vtnet5      -> v4: 10.10.50.1/32
OPT5 (opt5)    -> vtnet6      -> v4: 10.10.90.1/32

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

Enter an option: █

```

Une fois pfSense redémarré, le menu console s'affiche. Ce menu permet des actions essentielles comme : configurer les interfaces IP, réinitialiser le mot de passe, redémarrer le système ou encore accéder au shell FreeBSD.

Interface console de pfSense

Une fois pfSense démarré, un menu d'administration en ligne de commande s'affiche. Ce menu permet de réaliser différentes actions de configuration de base, utiles notamment en cas de problème d'accès à l'interface web.

Voici les options principales :

- 1) Assign Interfaces : Modifier les interfaces WAN et LAN
- 2) Set interface(s) IP address : Configurer une adresse IP manuellement
- 3) Reset webConfigurator password : Réinitialiser le mot de passe admin
- 5) Reboot system : Redémarrer pfSense
- 8) Shell : Accéder au terminal FreeBSD en ligne de commande

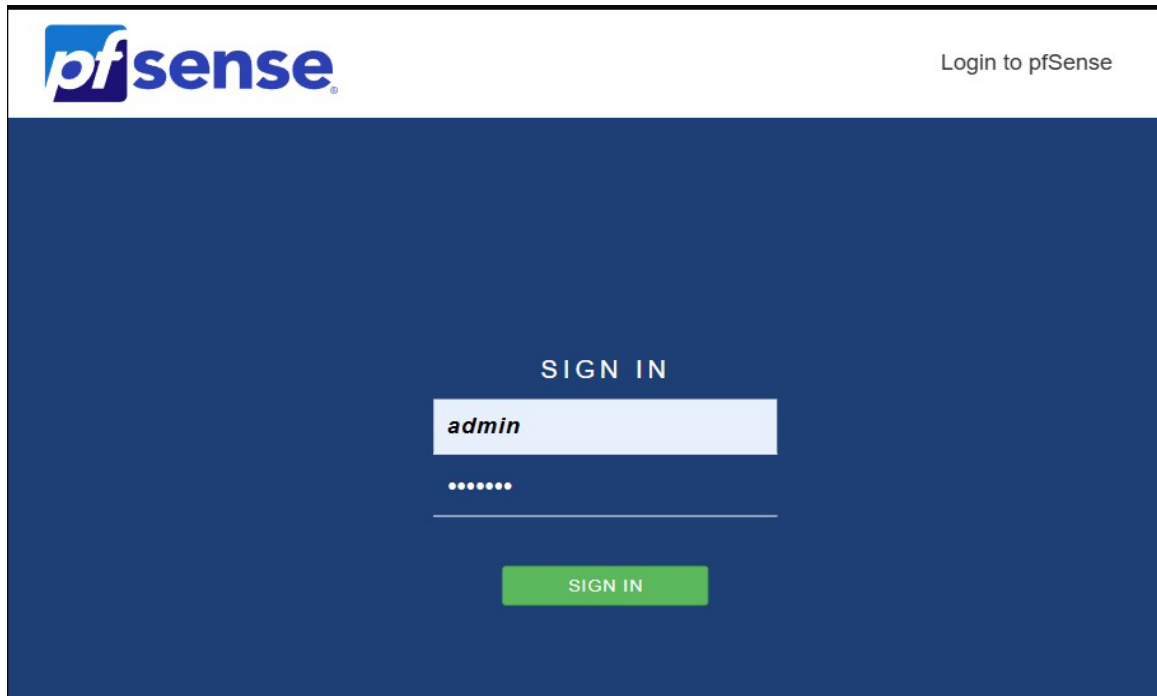
Ce menu peut être consulté directement depuis la VM (Proxmox) ou physiquement si pfSense est installé sur une machine dédiée.

Benjamin MANOLIOS

II. Configuration de pfSense

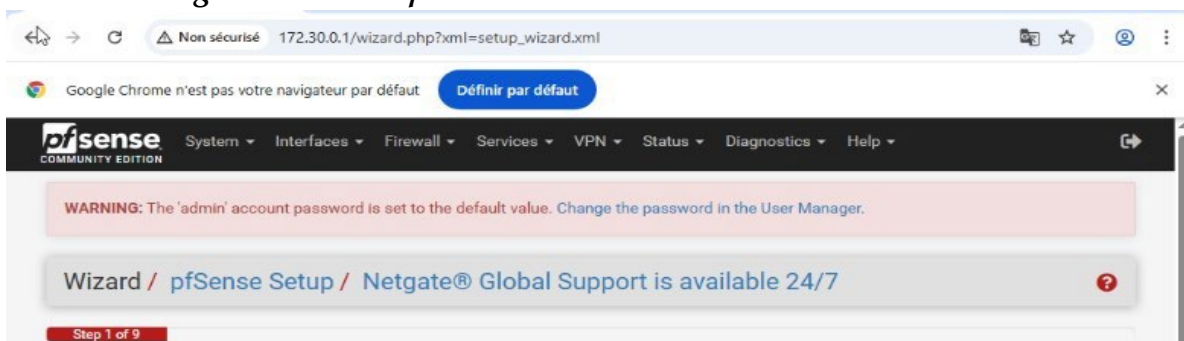
Configuration web

a- Connexion à l'interface web :



Cette page correspond à l'interface de connexion web de pfSense. On y accède via un navigateur web en saisissant l'adresse IP locale (ici <https://172.30.0.1>). Par défaut, l'identifiant est admin et le mot de passe est pfsense. Cette étape permet d'accéder à l'ensemble de la configuration via une interface graphique.

b- Changement mot de passe :



Une fois connecté, nous accédons à la section "User Manager" afin de modifier le mot de passe administrateur via l'option "Change the password".

Benjamin MANOLIOS

System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

User Properties

Defined by SYSTEM

Disabled ☐ This user cannot login

Username admin

Password

Full name System Administrator
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

Not member of

Member of admins

[Move to "Member of" list](#) [Move to "Not member of" list](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Nous remplaçons ensuite le mot de passe administrateur par un mot de passe sécurisé, puis nous validons la modification en cliquant sur le bouton "Save" en bas de la page.

pfSense.home.arpa - Interfaces x pve3 - Proxmox Virtual Environ x

Non sécurisé 172.30.0.1/interfaces.php?if=opt5

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / OPT5

The OPT5 configuration has been changed. The changes must be applied. Don't forget to adjust the DHCP settings after applying.

Apply Changes

General Configuration

Enable ☐

Description OPT5
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

Conclusion

Ce projet de mise en place d'un pare-feu pfSense au sein de la Maison des Ligues de Lorraine (M2L) s'est inscrit dans une démarche de **renforcement de la sécurité réseau** et de **modernisation de l'infrastructure informatique**. Avant cette réalisation, le réseau de la M2L souffrait d'un manque de segmentation, d'un routage centralisé insuffisant, ainsi que d'une absence de règles de sécurité précises, ce qui exposait l'infrastructure à des risques importants.

En installant et configurant pfSense sur un environnement virtualisé via **Proxmox VE**, j'ai pu proposer une solution fiable, évolutive et économique, qui répond aux besoins de l'organisation. Cette solution a permis :

La **création de VLANs** pour segmenter les flux réseau selon les usages (serveurs, postes clients, etc.) ;

L'**attribution dynamique des adresses IP** grâce à un serveur DHCP interne ;

La mise en place de **règles de filtrage précises** pour contrôler les accès entre les différentes zones ;

La séparation entre les zones sensibles comme la **DMZ** et le **réseau interne**, garantissant une meilleure protection des données.

Cette infrastructure offre à la M2L une meilleure visibilité sur le trafic, une plus grande flexibilité en cas d'ajout de nouvelles machines ou services, et un **niveau de sécurité renforcé**, tout en restant accessible grâce à l'interface web intuitive de pfSense.

Sur le plan personnel, ce projet m'a permis de **mobiliser plusieurs compétences clés** du référentiel BTS SIO option SISR :

L'installation et la gestion de machines virtuelles (hyperviseur Proxmox)

La configuration d'un pare-feu open source avancé (pfSense)

La gestion des VLANs et des plans d'adressage IP

La mise en œuvre de règles de sécurité réseau adaptées aux besoins métiers

Au-delà des compétences techniques, ce projet m'a également permis de développer ma **rigueur**, mon **autonomie**, et ma **capacité d'analyse**, des qualités essentielles dans les métiers de l'administration système et réseau.

En conclusion, cette réalisation constitue une **expérience professionnelle enrichissante**, concrète et représentative des missions qu'un technicien SISR peut être amené à gérer. Elle m'a permis de contribuer à la sécurité d'une véritable organisation tout en renforçant mes compétences techniques et méthodologiques dans un contexte professionnel.

ANNEXE BTS :

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS		SESSION 2025
ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)		
Épreuve E6 - Administration des systèmes et des réseaux (option SISR)		

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE		N° réalisation : 01
Nom, prénom : MANOLIOS Benjamin		N° candidat : 02443855566
<input checked="" type="checkbox"/> Épreuve ponctuelle <input type="checkbox"/> Contrôle en cours de formation		Date :
Organisation support de la réalisation professionnelle La Maison des Ligues de la Lorraine, établissement du Conseil Régional de Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d'autres structures hébergées. La M2L doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées. Elle assure l'offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région. M2L souhaite mettre en place un routeur virtuel pour gérer ses réseaux.		
Intitulé de la réalisation professionnelle		
Installation et configuration d'un routeur pfSense		
Période de réalisation : 01/10/2024 - 22/11/24		Lieu : EPSI MONTPELLIER
Modalité : <input type="checkbox"/> Seul <input checked="" type="checkbox"/> En équipe		
Compétences travaillées		
<input checked="" type="checkbox"/> Concevoir une solution d'infrastructure réseau <input checked="" type="checkbox"/> Installer, tester et déployer une solution d'infrastructure réseau <input checked="" type="checkbox"/> Exploiter, dépanner et superviser une solution d'infrastructure réseau		
Conditions de réalisation ¹ (ressources fournies, résultats attendus)		
Ressources fournies :		Résultats attendus :
<ul style="list-style-type: none"> • Cahier des charges M2L • Serveur Asus PRO Q570M • Proxmox VE 8.2 • ISO pfSense • VM client Linux/Windows 		<ul style="list-style-type: none"> • Gestion des réseaux • Filtrage par les règles de sécurité • Sécurisation des réseaux (pare-feu)
Description des ressources documentaires, matérielles et logicielles utilisées ²		
<ul style="list-style-type: none"> • Schéma réseau M2L • Documentation d'installation et configuration de pfSense • Documentation d'installation et configuration de VM client Linux/Windows • Documentation d'installation et configuration de Proxmox VE 		
Modalités d'accès aux productions et à leur documentation		
Lien de production : Insh.xyz/ed11ef		
Lien de documentations :		
<ul style="list-style-type: none"> • pfSense : Insh.xyz/0690a7 • Proxmox : Insh.xyz/ddf77c • Client : Insh.xyz/48f056 		

¹ En référence aux conditions de réalisation et ressources nécessaires du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.

² Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

³ Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

⁴ Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.