N°candidat : 02045677973
TARASSE Saossane

EPSI Montpellier
BTS SIO SISR 2024/2025

Epreuve E6
Situation N°1

Segmentation du réseau

Mise en place des VLANS sur le coeur du réseau

Table de matière:

Contexte: Maison des Ligues de Lorraine **3**
Besoins **3**
Objectifs du projet **4**
Choix Techniques: 5
Avantages: 5
Inconvénients: 5
Explication de la solution proposée: **6**
Création des VLANs et des vmbr associé sur proxmox 8
Création des vlans sur PFsense 9
Connexion au switch D-link 12
Création de lien trunk entre les 2 switchs 13
Routage inter-vlan 13
Conclusion **14**
Annexe **14**

Contexte: Maison des Ligues de Lorraine

La Maison des Ligues de Lorraine (M2L) est un établissement sous l'égide du Conseil Régional de Lorraine, ayant pour mission principale d'assurer la gestion et le support des ligues sportives régionales ainsi que d'autres structures hébergées.

Afin de garantir un fonctionnement optimal et sécurisé, la M2L met à disposition des infrastructures adaptées, incluant des ressources matérielles et logistiques, permettant aux ligues de bénéficier d'un environnement stable et performant.

Dans cette optique, la M2L souhaite moderniser et centraliser la gestion de son infrastructure informatique. Cette modernisation vise à simplifier l'administration des utilisateurs, la gestion des adresses IP et le déploiement d'applications au sein de son réseau.
En adoptant une solution intégrée et automatisée, la M2L aspire à renforcer la sécurité, optimiser la gestion des accès et faciliter l'organisation des ressources informatiques pour les ligues sportives qu'elle héberge.

Besoins

- Séparer les flux réseaux des différentes **ligues sportives hébergées**.
- Isoler les **services administratifs** internes de la M2L.
- Prévoir un VLAN pour les **visiteurs ou intervenants externes**.

Sécurité et contrôle d'accès

- Éviter que des utilisateurs non autorisés accèdent à des ressources critiques.
- Permettre uniquement la communication intra-VLAN
- Filtrage des communications selon le rôle.

Optimisation du trafic réseau

- Réduire les domaines de broadcast.
- Améliorer la performance réseau en isolant les communications inutiles entre différents services.

Facilité de gestion et évolutivité

- Simplifier le **déploiement d'applications** en les affectant à des VLAN spécifiques (ex: GLPI sur VLAN 20)
- Centraliser la **gestion IP** avec un plan d'adressage structuré par VLAN.

Objectifs du projet

Ce projet vise à améliorer la gestion et la segmentation du réseau en mettant en place des VLANs sur le cœur du réseau de l'organisation. L'objectif est de renforcer la sécurité, optimiser les performances et assurer une meilleure administration des ressources réseau.

Segmentation du réseau à l'aide de VLANs pour isoler les différents services et améliorer la sécurité.

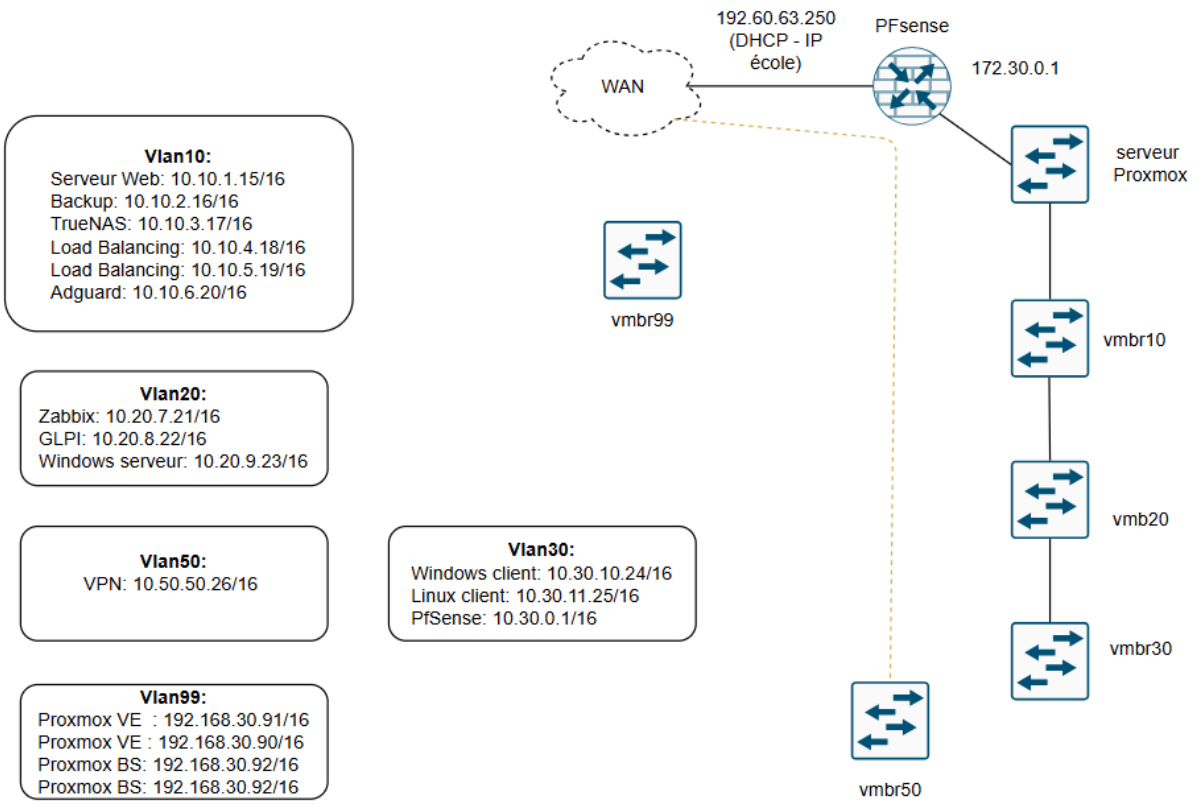
Configuration des switches pour assurer l'interconnexion des VLANs et le routage adéquat.

Mise en place du routage inter-VLAN pour permettre la communication entre les différents segments du réseau via un routeur ou un firewall.

Attribution dynamique des adresses IP via DHCP en fonction des VLANs.

Sécurisation du réseau avec des ACLs (Listes de contrôle d'accès) et le filtrage des accès.

Gestion centralisée des équipements réseau à travers une solution d'administration adaptée.



Choix Techniques:

Avantages:

Isolation des services: Les VLANs séparent les flux réseau empêchant les appareils du VLAN 10 de communiquer directement avec le VLAN 20. Ce qui permet d'éviter la propagation des menaces.

Réduction de broadcast: La création de VLANs va permettre une amélioration des performances en réduisant les domaines de broadcast. Autrement dit, les portes du switch ne seront pas inondées de messages. Tous les appareils qui sont connectés sur le même réseau local, plus précisément ceux qui partagent le même segment IP, ne recevront pas les messages des autres appareils qui ne sont pas dans le même domaine de diffusion.

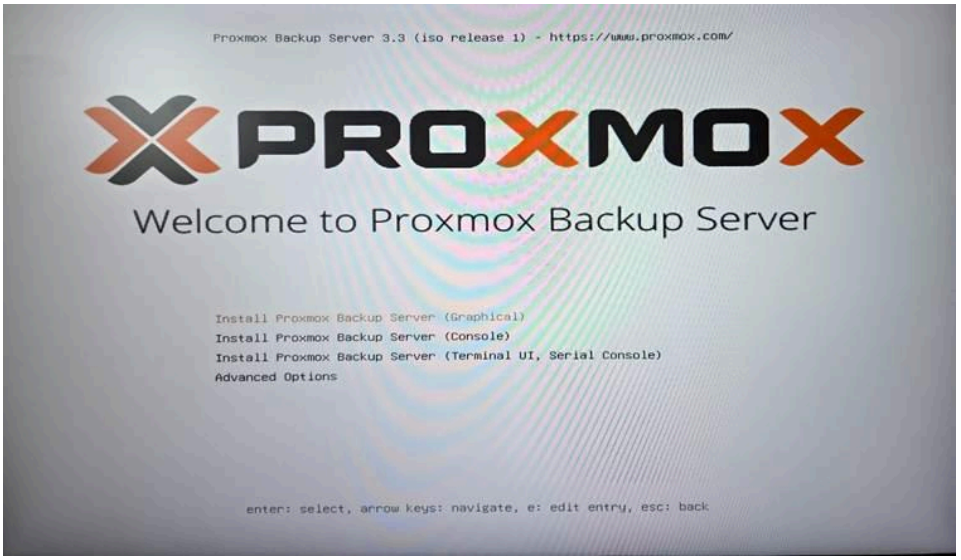
Gestion centralisée: Permet un déploiement homogène des politiques de sécurité.

Inconvénients:

Configuration: Une mauvaise configuration des liens **trunks** peut bloquer le trafic VLAN.
VLAN 1 (VLAN par défaut) transporte les trames non taguées ce qui crée un risque si un attaquant se connecte.
Un port configuré en mode access (sans tag) au lieu de trunk (tagué) bloque le trafic inter-vlan.

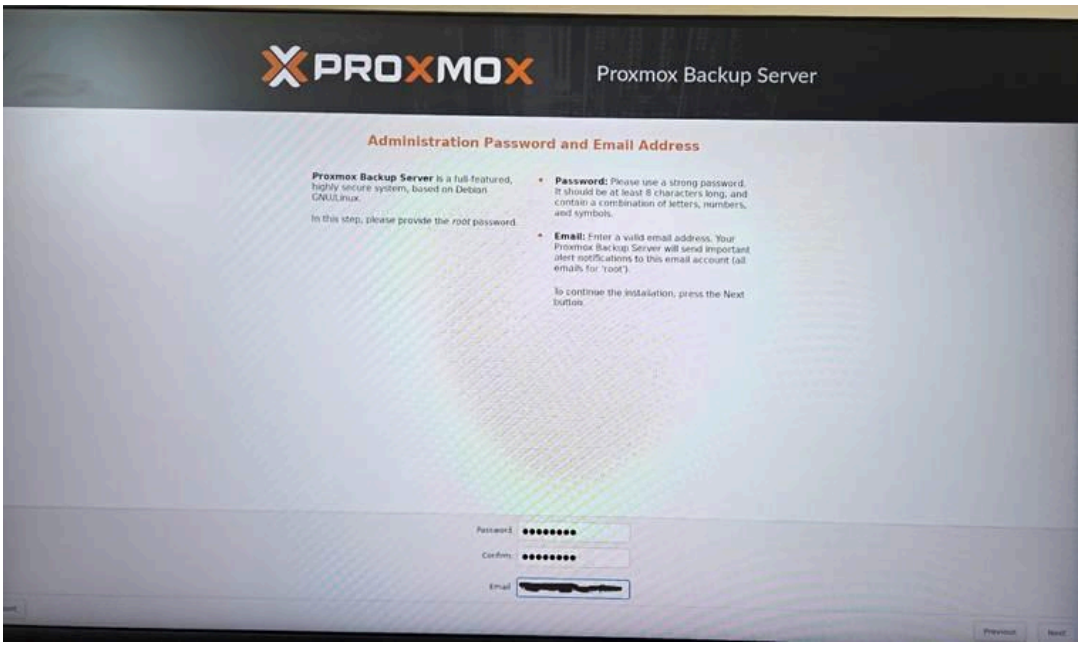
Explication de la solution proposée:

Installation Proxmox Backup server:

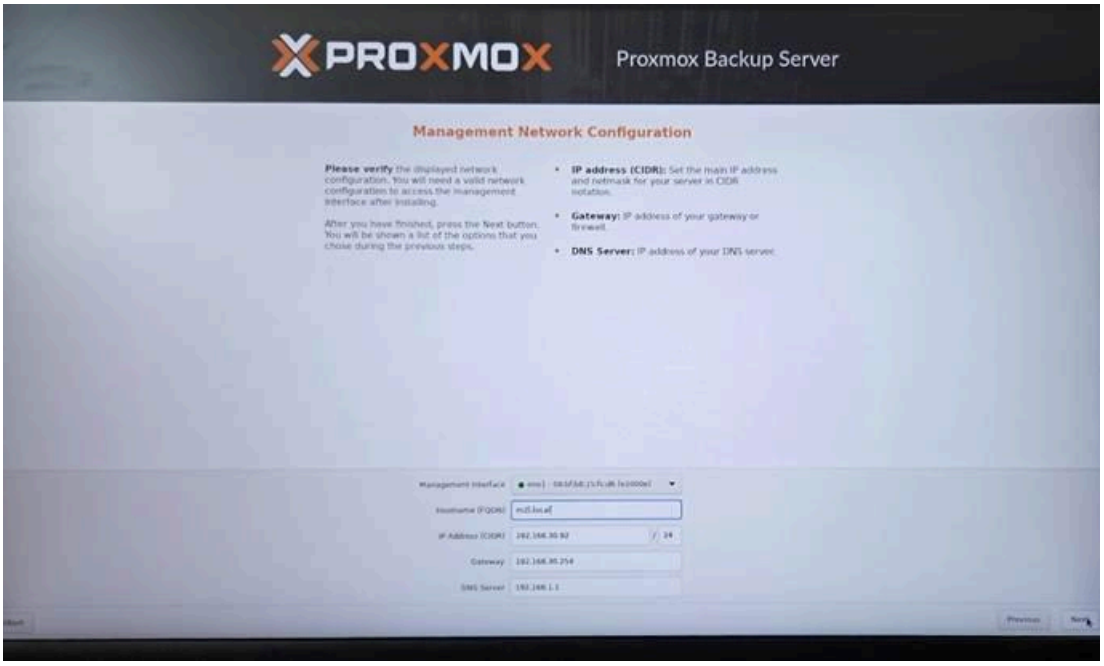


Pour cette installation j'ai choisi de prendre ***« Install Proxmox Bakcup Server (Graphical)*** », car plus simple et rapide.

On choisit un disque ou une machine qu'on souhaite avoir en backup.



Nous choisissons un mot de passe avec une adresse mail qui nous servira pour le serveur backup qui nous enverra diverses notifications importantes.

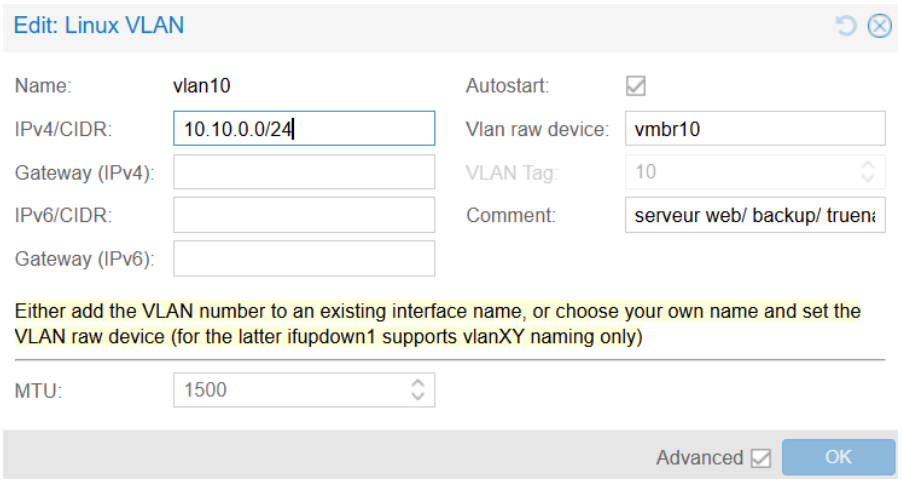


On choisi l'adresse IP la dans ce cas nous allons prendre, ***192.168.30.92/24,*** avec une Gateway ***192.168.30.254*** ainsi qu'un DNS ***192.168.1.1***

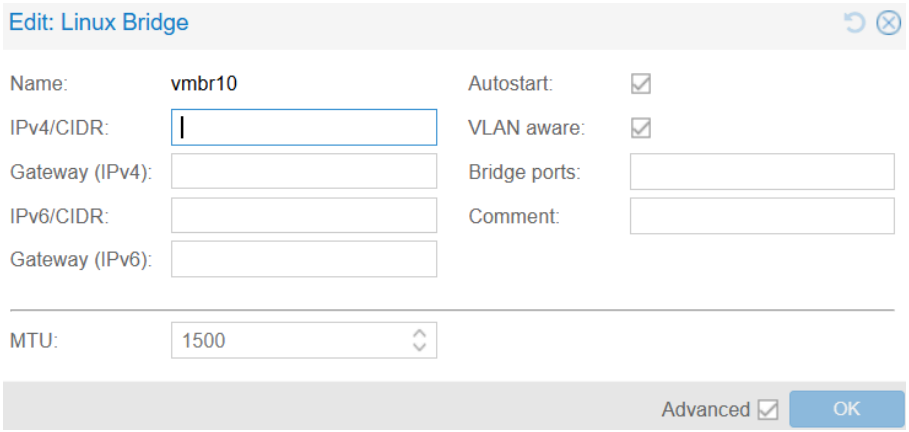
Une fois l'installation terminée, un message s'affiche pour confirmer la réussite de l'installation avec également l'adresse IP de notre Proxmox à savoir 192.168.30.92:8007

Création des VLANs et des vmbr associé sur proxmox

Les VLANs servent à segmenter et organiser des machines de façon flexible et sécurisée. Les vmbr agissent comme des commutateurs virtuels.
En associant un VLAN spécifique à un vmbr, on permet à chaque VM de rejoindre le bon segment réseau.



Tout d'abord, nous allons créer un VLAN 10 auquel nous allons attribuer une IP et un vmbr (un bridge virtuel).
Pour faciliter la gestion, nous avons associé un VLAN 10 à un vmbr10. Le même numéro est utilisé pour simplifier l'identification.
J'ai ajouté un commentaire sur chaque VLAN indiquant les VM qui y sont associées.



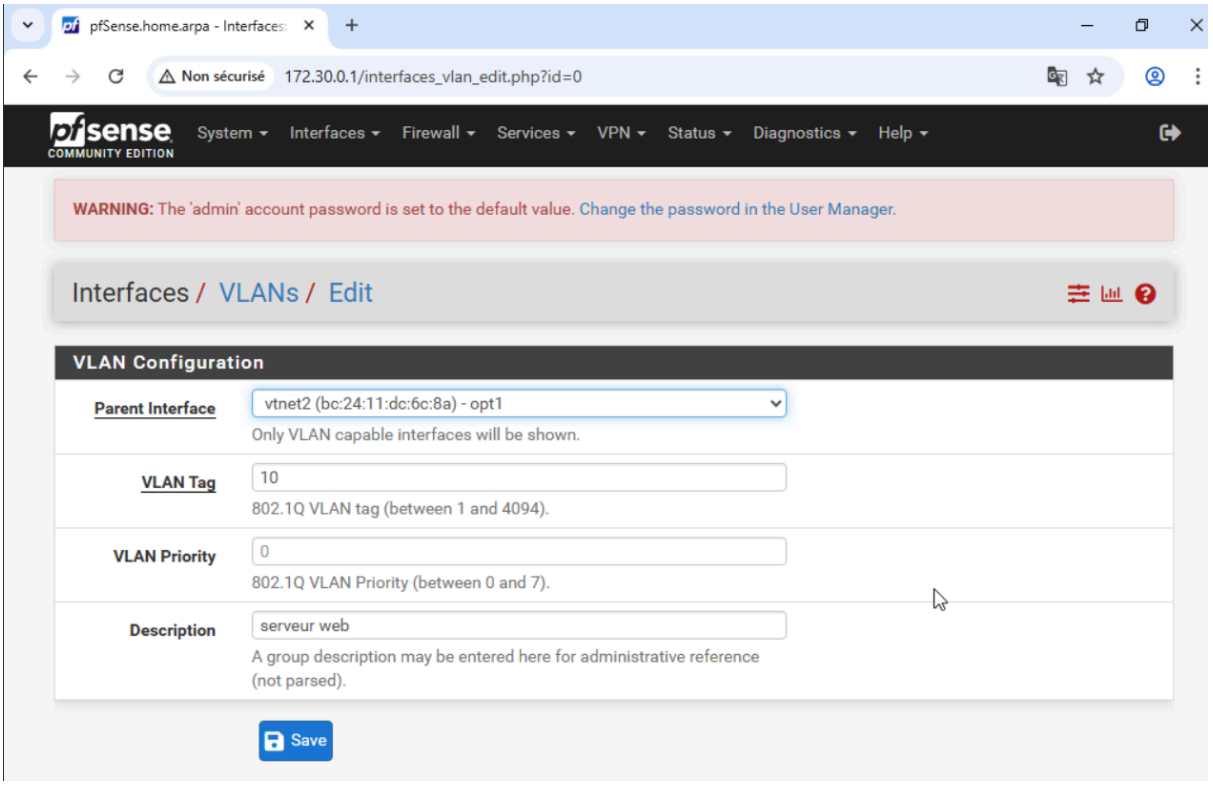
On crée ensuite notre bridge que l'on va associer au VLAN.
Il n'est pas nécessaire de configurer une IP ici. En cochant la case 'VLAN aware', le bridge héritera automatiquement de l'IP définis au niveau du VLAN.

vlan10	Linux VLAN	Yes	Yes	No	10.10.0.0/24	serveur web/ backup/ truenas/ loadbalancing/ adguard
vlan20	Linux VLAN	Yes	Yes	No	10.20.0.0/24	zabbix/ glpi/ windows serveur
vlan30	Linux VLAN	Yes	Yes	No	10.30.0.0/24	client linux / windows
vlan50	Linux VLAN	Yes	Yes	No	10.50.50.0/24	vpn
vlan99	Linux VLAN	Yes	Yes	No	192.168.30.0/24	proxmox
vmbr0	Linux Bridge	Yes	Yes	No	192.168.30.90/24	
vmbr1	Linux Bridge	Yes	Yes	No		
vmbr10	Linux Bridge	Yes	Yes	Yes		
vmbr20	Linux Bridge	Yes	Yes	Yes		
vmbr30	Linux Bridge	Yes	Yes	Yes		
vmbr50	Linux Bridge	Yes	Yes	Yes		
vmbr99	Linux Bridge	Yes	Yes	Yes		

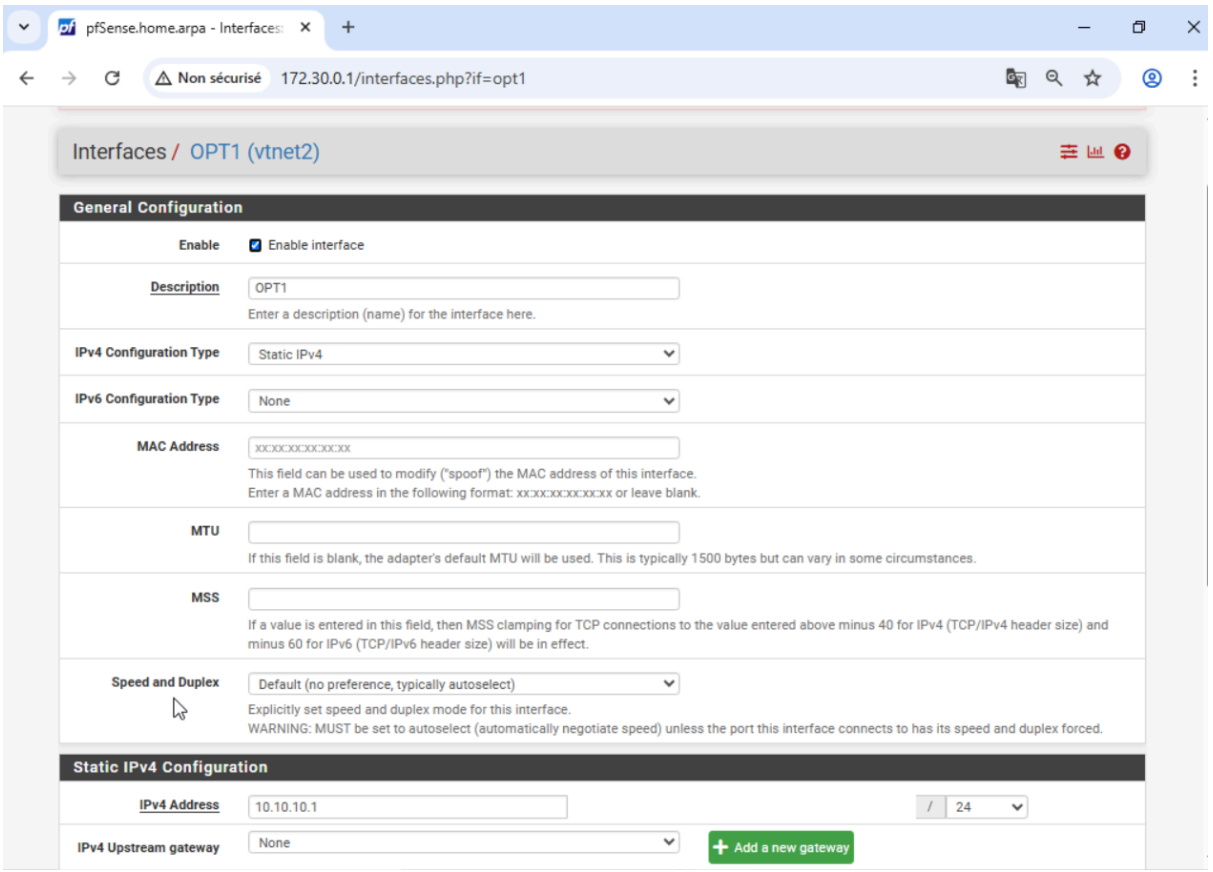
Tous les VLANs et vmbr doivent bien être activés.

Création des vlans sur PFsense

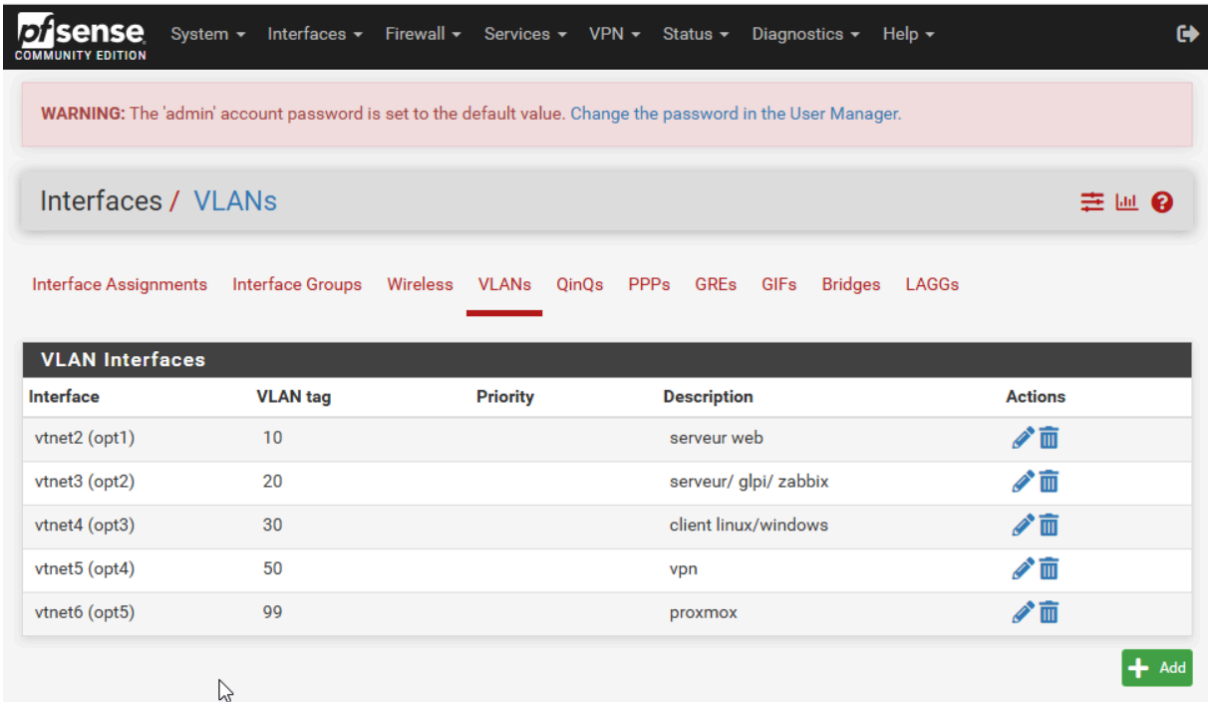
Nous allons aller dans la rubrique ‘interfaces’, ‘Assignments’, c’est ici que nous allons pouvoir créer tous nos VLANs que l’on va associer à un vtnet.
Un vtnet correspond à une interface du réseau virtuel dans PfSense.
Elle représente les cartes réseaux de la machine virtuelle.
Ces interfaces permettent à PfSense de communiquer avec les VLANs via les bridges de Proxmox.



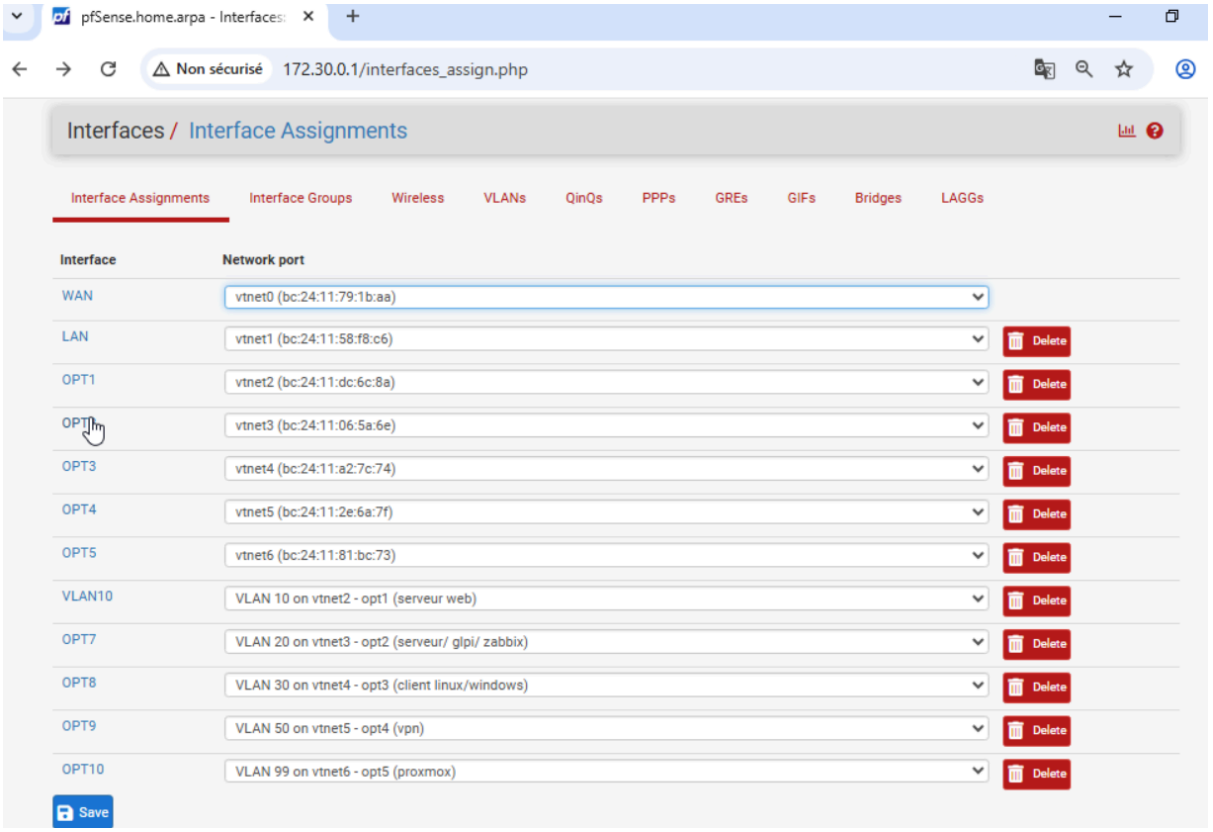
Dans un premier temps, nous allons créer nos VLANs en les attribuant à une interface vtnet de PfSense.



Avant d'appliquer les modifications ou ajouter un VLAN à une interface, il faut bien vérifier l'IP attribué au vtnet afin de savoir si elle correspond bien à l'IP attribué au VLAN sur notre Proxmox.



On vérifie que tous les VLANs ont bien été créés. On leur associe une description pour pouvoir mieux gérer les interfaces.



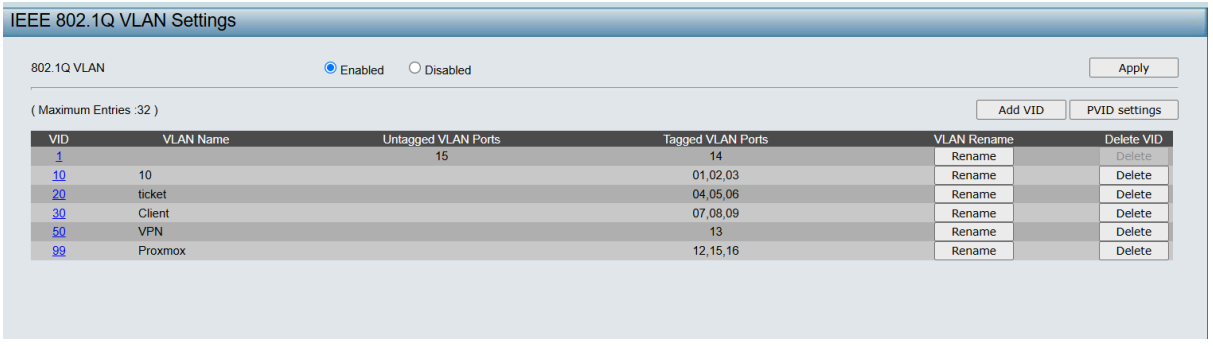
On active les interfaces que l'on vient de créer sur le PfSense, qui seront visibles et supprimables en cas de mauvaise configuration.

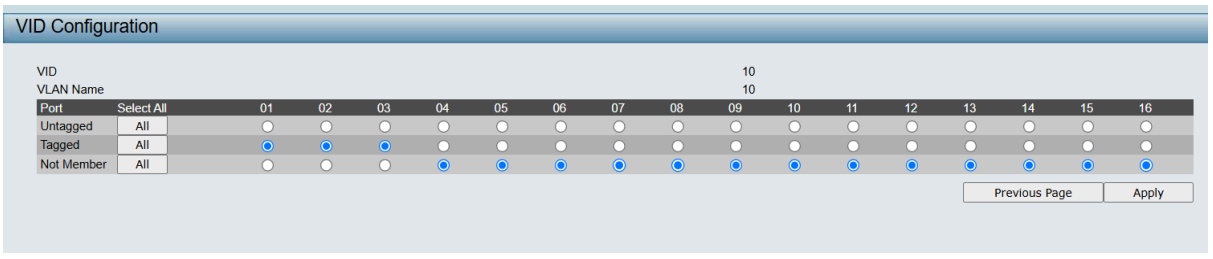
Connexion au switch D-link

Tout d'abord nous allons configurer l’adresse ip et le masque de sous-réseau du PC pour permettre la connexion

Nous arrivons sur l’interface de notre switch

Pour créer les VLANs, nous allons aller dans la rubrique VLANs puis 802.1Q





Création de lien trunk entre les 2 switchs

Un lien trunk est nécessaire pour faire passer plusieurs VLANs sur un même câble.

Aller sur l'interface 'VLAN interface settings' aller sur le port où l'on souhaite créer la liaison (ex: port 14). Configurer les VLANs en mode 'Tagged'.

Tagged VLANs signifie que le port va transmettre les trames de ces VLANs en ajoutant une étiquette (un tag 802.1Q) qui indique à quel VLAN chaque trame appartient.

En ajoutant des VLANs dans cette liste, on autorise le port à faire passer le trafic des VLANs.

Le fait que plusieurs VLANs soit en mode tagged sur le port suffit à faire office de trunk.

Cependant, parfois des trames arrivent sans étiquette dite 'non-taggé' ou 'untagged', le switch va les placer automatiquement dans le VLAN natif (par défaut), généralement le VLAN 1.

Le VLAN natif va servir à ranger automatiquement le trafic qui circule sur le trunk sans étiquette pour qu'il ne soit pas perdu et bien traité sur le réseau.

Répéter la configuration sur l'autre switch

en cours de réalisation

Routage inter-vlan

Le routage inter-vlan permet à des appareils de VLANs différents de communiquer entre eux, grâce à un appareil qui fait du routage (switch L3).

Sans cette configuration, les VLANs seront isolés, autrement dit, les appareils d'un VLAN 10 par exemple ne pourront pas communiquer avec les appareils présents sur le VLAN 20.

Pour cela nous aurons besoin de nos switchs sur lesquels nous avons configuré les VLANs et où nous avons assigné des ports aux VLANs.

Pour faire passer plusieurs VLANs en même temps sur un même câble réseau, nous allons utiliser l'encapsulation dot1Q, qui sert à 'taguer' les paquets.

On va créer des sous-interface virtuelle nommée 0.10 par exemple pour le VLAN 10 et à l'aide de la commande 'encapsulation dot1Q 10', nous allons expliquer que cette sous-interface utilise le VLAN 10.

Puis donner une IP à cette sous-interface, l'adresse de passerelle pour tous les appareils du VLAN 10.

Dans un premiers temps, nous allons activer le routage IP en réalisant la commande 'ip routing', qui permettra de faire circuler des paquets de données entre plusieurs réseaux différents

en cours de réalisation

Conclusion

La mise en place des VLANs au sein de l'infrastructure réseau de la Maison des Ligues de Lorraine a permis d'apporter une segmentation claire, sécurisée et adaptée aux besoins spécifiques des différents services hébergés.
A l'aide des outils comme Proxmox, pfSense et les switchs D-Link, on a pu segmenter efficacement le réseau, ce qui a contribué à une meilleure isolation des flux, une réduction des risques de sécurité et une optimisation des performances globales du réseau.

Le déploiement du routage inter-VLAN a permis d'assurer une communication contrôlée entre les VLANs, tout en maintenant des règles strictes de filtrage et de gestion des accès.
Cette solution flexible et évolutive pose les bases d'un réseau plus fiable**,** elle pourra facilement s'adapter aux futurs projets ou à l'ajout de nouveaux services.

Annexe

- **annexe 7: attestation du cahier décharge (après)**

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation** : 01
Nom, prénom : Saossane TARASSE	**N° candidat** : 02045677973
☑ **Épreuve ponctuelle** ☐ **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 une solution pour segmenter son réseau

Intitulé de la réalisation professionnelle
Mise en place des VLANS sur le coeur du réseau

Période de réalisation : 23/09/2024 - 19/11/2024 **Lieu :** EPSI MONTPELLIER

Modalité : ☐ Seul ☑ En équipe

Compétences travaillées
- ☑ Concevoir une solution d'infrastructure réseau
- ☑ Installer, tester et déployer une solution d'infrastructure réseau
- ☑ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation [1] (ressources fournies, résultats attendus)

Ressources fournies :
- Cahier des charges M2L
- Serveur Asus Pro Q570M
- Proxmox VE 8.2
- Switch D-link x2

Résultats attendus :
- segmentation de réseau
- sécurisation des accès

Description des ressources documentaires, matérielles et logicielles utilisées [2]
- Schéma réseau M2L, tableau des VLANS
- Documentation d'installation et configuration de Proxmox VE
- Documentation d'installation et configuration de switch

Modalités d'accès aux productions [3] **et à leur documentation**
Lien de production : https://skullburn84.github.io/Portfolio/documentation.html
Lien de documentations :
- **VLAN** : https://skullburn84.github.io/Portfolio/vlan
- **pfSense** : https://skullburn84.github.io/Portfolio/pfsense
- **Proxmox** : https://skullburn84.github.io/Portfolio/proxmox