

Documentation  
d'installation  
configuration des bornes  
WIFI + portail captif



DOCUMENTATION  
**BANANE**  
**Mohamed**

---

BTS SIO SISR 2024/2025

# Sommaire

---

## **1.CONTEXTE**

PRÉSENTATION DE LA M2L ET DE SES OBJECTIFS.

## **2.PROBLÈME ET SOLUTION**

GESTION INEFFICACE DES INCIDENTS ET DES ÉQUIPEMENTS AVANT L'IMPLÉMENTATION DU PORTAIL CAPTIF ET DES BORNES WIFI, ET COMMENT CES SOLUTIONS RÉSOLVENT CES PROBLÈMES.

## **3.RÉSEAU AVANT MODIFICATION**

CONFIGURATION DU RÉSEAU AVANT L'AJOUT DU PORTAIL CAPTIF ET DES BORNES WIFI.

## **4.QU'EST-CE QU'UN PORTAIL CAPTIF ET DES BORNES WIFI ?**

INTRODUCTION AU PORTAIL CAPTIF ET AUX BORNES WIFI : GESTION DES ACCÈS, AUTHENTIFICATION DES UTILISATEURS, AMÉLIORATION DE LA CONNECTIVITÉ ET DE LA SÉCURITÉ.

## **5.RÉSEAU APRÈS MODIFICATION**

AJOUT DU PORTAIL CAPTIF ET DES BORNES WIFI AU RÉSEAU ET IMPACT SUR LA GESTION DES CONNEXIONS ET LA SÉCURITÉ.

## **6.INSTALLATION DU PORTAIL CAPTIF**

ÉTAPES DÉTAILLÉES POUR L'INSTALLATION ET LA CONFIGURATION D'UN PORTAIL CAPTIF SUR LE RÉSEAU.

## **7.CONNEXION À LA BORNE**

PROCÉDURE DE CONNEXION DES UTILISATEURS AUX BORNES WIFI VIA LE PORTAIL CAPTIF.

## **8.CONFIGURATION DE LA BORNE**

PARAMÉTRAGE ET OPTIMISATION DES BORNES WIFI POUR ASSURER UNE COUVERTURE RÉSEAU EFFICACE ET SÉCURISÉE.

## **9.CONCLUSION**

## **10.ANNEXE BTS**



# Le client

# Problème/Solution

---

## Client : Maison des Ligues de Lorraine (M2L)

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.

### Problème :

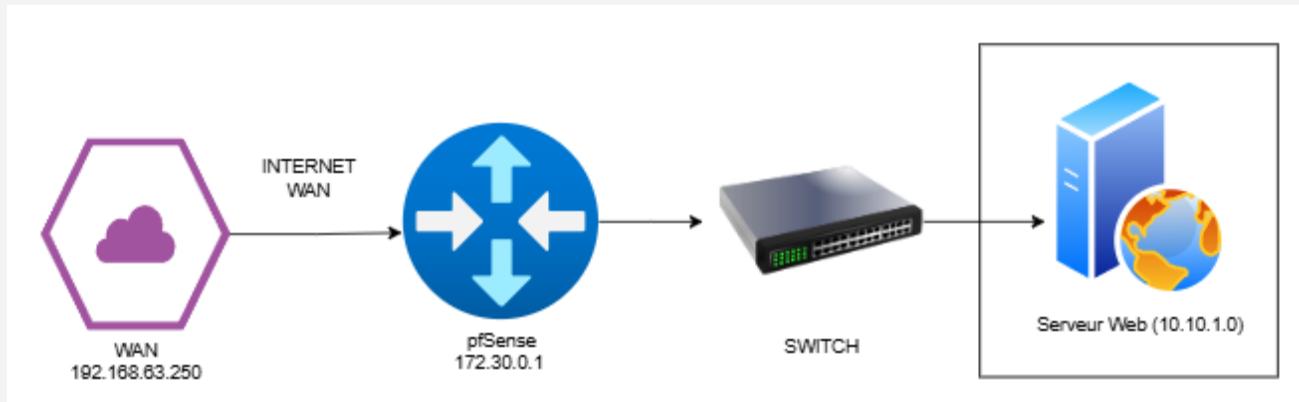
- La M2L souhaite moderniser son infrastructure WiFi en :
- Offrant un accès WiFi sécurisé et centralisé aux ligues et visiteurs.
- Contrôlant et authentifiant les utilisateurs via un portail captif.
- Optimisant la gestion des ressources réseau (bande passante, adresses IP, restrictions d'usage).

### Solution :

- Installation de bornes WiFi professionnelles (ex : Ubiquiti, Aruba, Cisco Meraki) pour une couverture optimale.
- Mise en place d'un contrôleur WiFi (physique ou cloud) pour gérer les bornes et le trafic.
- Création de plusieurs SSID (ex : "M2L-Staff", "M2L-Visiteurs") avec des règles de gestion spécifiques.
- Configuration d'un serveur DHCP pour l'attribution des adresses IP selon le profil utilisateur.
- Installation d'un portail captif pour forcer l'authentification des utilisateurs avant l'accès à Internet.



# Réseaux avant modification



Le réseau de la Maison des Ligues de Lorraine (M2L) était structuré sans la solution de gestion GLPI, et les différents services et équipements étaient répartis comme suit :

- **WAN (192.168.63.250)** : L'interface WAN, permettant la connexion à Internet, était située dans le réseau 192.168.63.0.
- **PfSense (172.30.0.1)** : Le pare-feu PfSense avait une adresse IP dans le sous-réseau 172.30.0.0, qui gérait la sécurité et les règles de filtrage pour les communications internes et externes.
- **Switch** : Le switch, assurant l'interconnexion des équipements réseau, était sur le sous-réseau 192.168.30.0/24, avec l'adresse 192.168.30.90.
- **Serveur Web (10.10.1.0)** : Le serveur web était connecté à VLAN 30 et utilisait des adresses IP dans le sous-réseau 10.10.1.0, permettant la communication avec les autres équipements du réseau.

# **Qu'est-ce qu'un portail captif et des bornes WiFi ?**

## **1. Qu'est-ce qu'un portail captif et des bornes WiFi ?**

### **Portail Captif**

Un portail captif est une solution réseau qui contrôle et sécurise l'accès à Internet en obligeant les utilisateurs à s'authentifier avant de pouvoir naviguer. Il est souvent utilisé dans les environnements professionnels, publics ou éducatifs pour filtrer les connexions, appliquer des règles d'accès et surveiller l'utilisation du réseau.

Principales fonctionnalités :

- Authentification des utilisateurs : Accès au réseau après validation via un identifiant/mot de passe, un code temporaire ou une authentification sociale.
- Sécurisation des connexions : Filtrage des contenus, blocage des sites non autorisés et gestion des droits d'accès.
- Traçabilité et logs : Enregistrement des connexions pour garantir une conformité légale et assurer une meilleure gestion du réseau.
- Personnalisation de l'accueil : Interface personnalisable avec des informations sur l'entreprise, des publicités ou des conditions d'utilisation.

### **Bornes WiFi / Access Points**

Les bornes WiFi (ou Access Points) sont des équipements permettant la diffusion d'un réseau sans fil à plusieurs utilisateurs dans une zone définie. Elles sont reliées au réseau filaire de l'entreprise et permettent une couverture optimale du signal WiFi.

Principales fonctionnalités :

- Extension du réseau : Permet d'offrir une connexion sans fil stable dans des bureaux, des espaces publics ou des bâtiments entiers.
- Séparation des accès : Différents SSID (réseaux WiFi distincts) peuvent être configurés pour les employés, les visiteurs et les appareils internes.
- Gestion centralisée : Surveillance et administration des points d'accès via un contrôleur ou une interface web.
- Optimisation des performances : Répartition automatique de la charge entre les bornes pour éviter les congestions réseau.

## **Pourquoi choisir un portail captif et des bornes WiFi pour une entreprise ?**

### **1. Sécurité renforcée**

Le portail captif assure que seuls les utilisateurs autorisés peuvent accéder au réseau, réduisant ainsi les risques de cyberattaques et de connexions indésirables.

### **2. Gestion efficace des connexions**

Grâce aux bornes WiFi, la couverture réseau est optimisée, et le portail captif permet une gestion avancée des accès (limitations de débit, horaires d'accès, authentification unique).

### **3. Traçabilité et conformité**

L'entreprise peut enregistrer les connexions pour respecter les obligations légales et surveiller l'utilisation du réseau sans compromettre la confidentialité des utilisateurs.

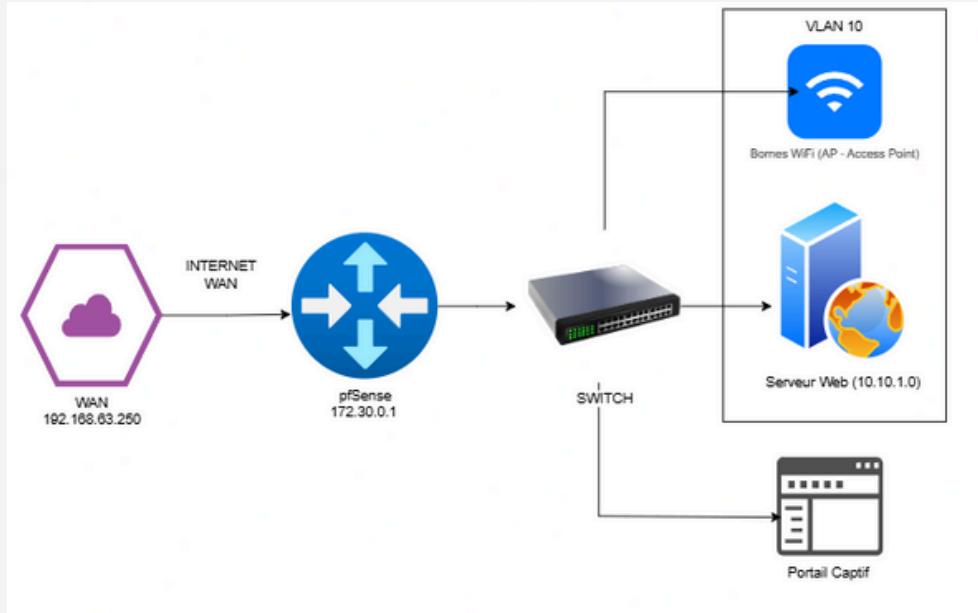
### **4. Expérience utilisateur améliorée**

L'accès au WiFi est simplifié avec une page d'accueil intuitive, des options de connexion rapide et une gestion fluide du trafic.

### **5. Adaptabilité et évolutivité**

Les solutions de portail captif et de bornes WiFi sont personnalisables selon les besoins de l'entreprise et évoluent facilement avec l'expansion des infrastructures.

# Réseaux après modification



Après l'implémentation du portail captif et des bornes WiFi (Access Points) dans le réseau, une nouvelle plage d'adresses a été attribuée pour le serveur web, et des améliorations ont été apportées à la gestion du réseau :

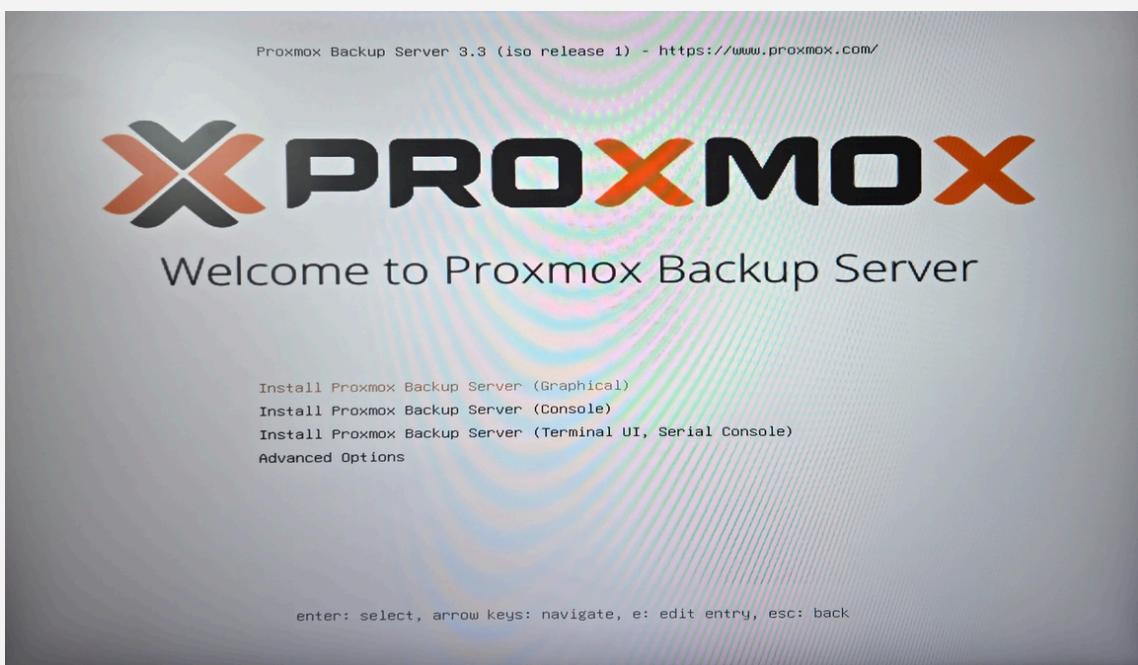
- **WAN (192.168.63.250)** : L'interface WAN reste inchangée, permettant toujours la connexion à Internet.
- **PfSense (172.30.0.1)** : Le pare-feu PfSense continue de gérer les règles de sécurité et le filtrage, mais maintenant avec une meilleure gestion de la communication vers le portail captif.
- **Switch** : Le switch reste sur le sous-réseau 192.168.30.0/24, permettant une interconnexion centralisée et efficace des équipements réseau.
- **Serveur Web (VLAN 10 - 10.10.1.0)** : Le serveur web est situé dans le sous-réseau 10.10.1.0, facilitant l'accès aux services internes.
- **Portail Captif** : Une nouvelle plage d'adresses 10.20.3.0/29 a été réservée pour le portail captif, qui gère l'authentification des utilisateurs avant l'accès au réseau. Ce sous-réseau permet de sécuriser les connexions et de contrôler les accès aux ressources de l'entreprise.
- **Bornes WiFi ( Access Points - VLAN 10)** : Les bornes WiFi sont déployées sur le VLAN 40, offrant une connexion sans fil sécurisée aux employés et aux visiteurs. Elles sont configurées pour fonctionner avec le portail captif, assurant une authentification obligatoire avant l'accès à Internet.

Grâce à cette infrastructure, le réseau est désormais mieux structuré pour gérer les connexions WiFi, l'authentification des utilisateurs et la gestion des accès, améliorant ainsi la sécurité et la performance du réseau pour la M2L et ses ligues sportives.

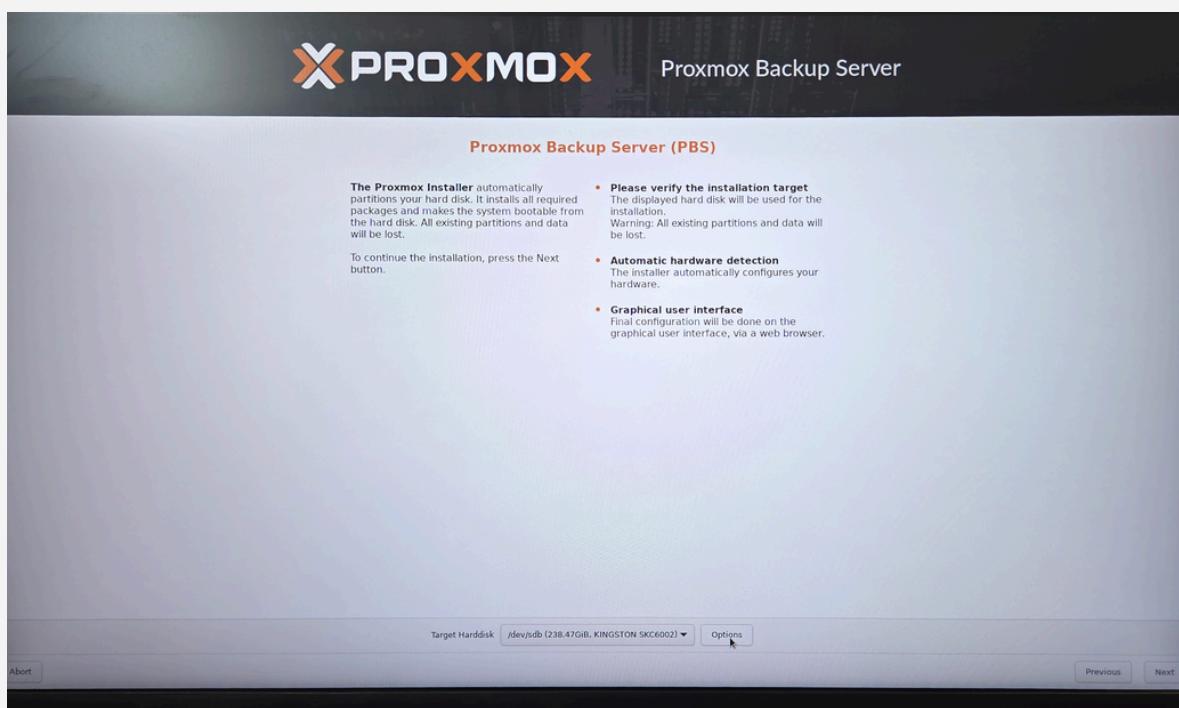


# Installation de Proxmox

Une fois la clé USB bootable créée, insérez-la dans un port USB de la machine sur laquelle vous souhaitez installer Proxmox et réglez le Bios pour qu'il démarre sur la clé USB ; l'assistant d'installation de Proxmox 8 s'affiche :

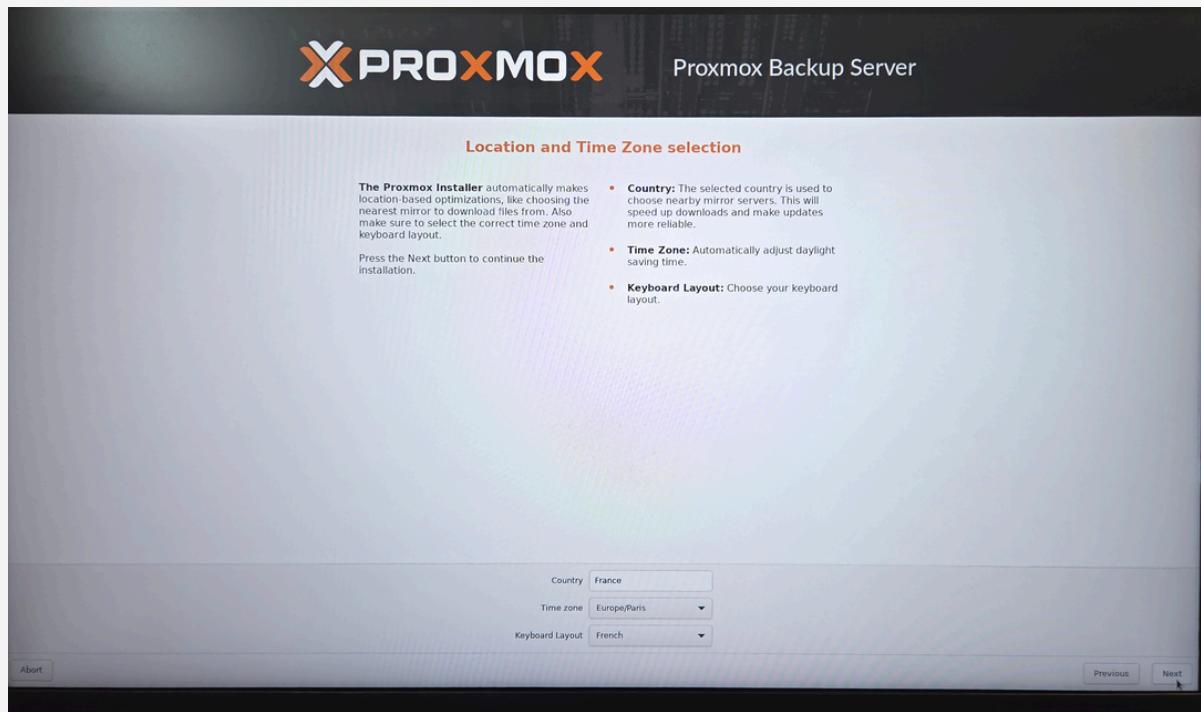


Sélectionnez, dans la fenêtre suivante, le disque sur lequel le système sera installé et cliquez le bouton « Suivant » :

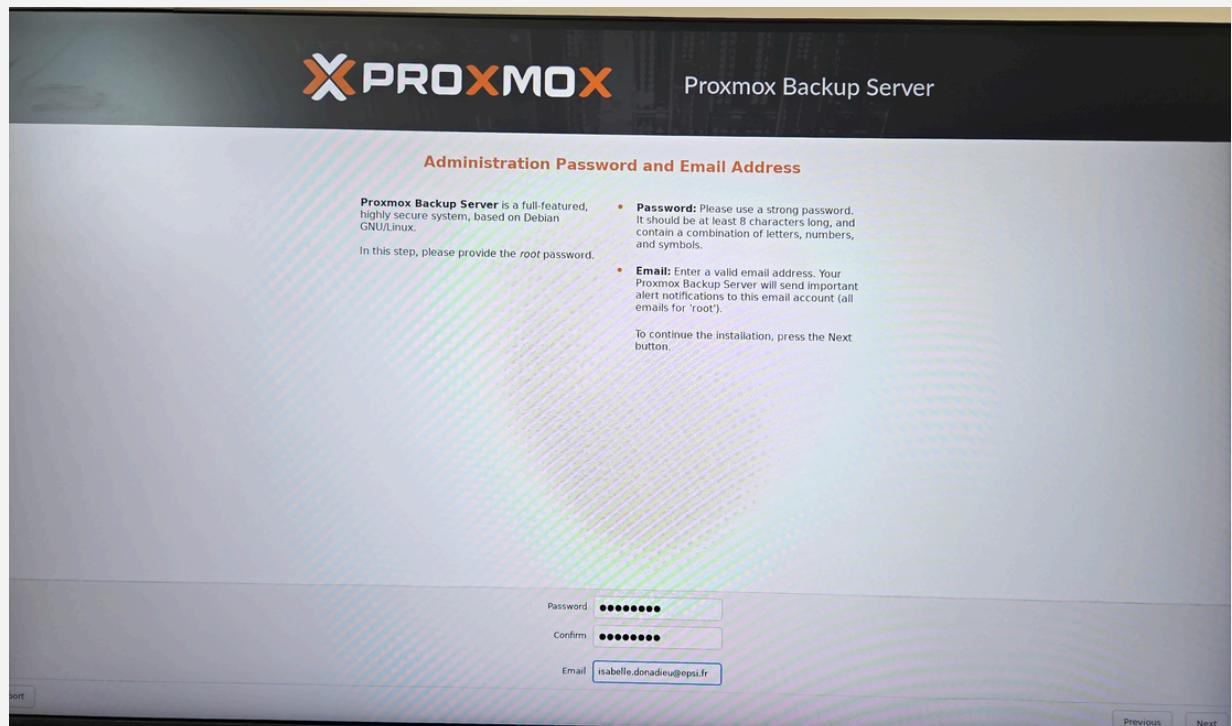


# Installation de Proxmox

Dans la rubrique « Country », saisissez « France » et cliquez le bouton « Next » :

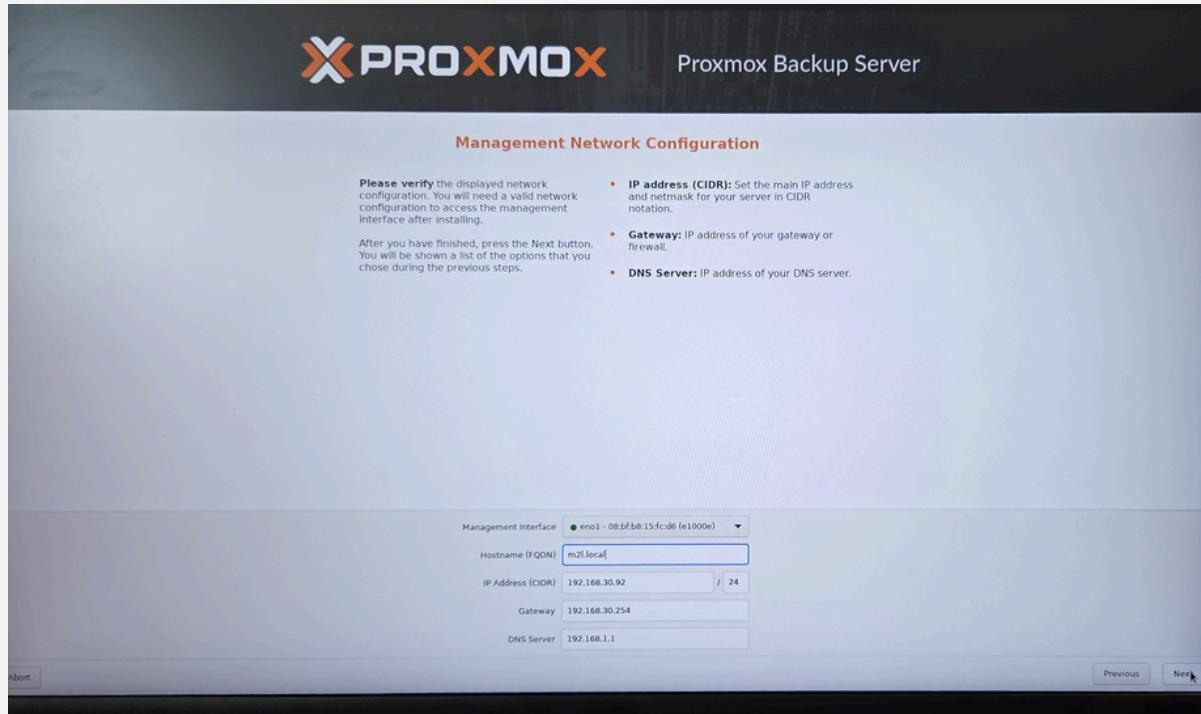


Saisissez le mot de passe qui sera attribué au compte « root » (super utilisateur) de Proxmox et indiquez un compte mail valide (qui vous permettra de recevoir différentes notifications en lien avec votre serveur Proxmox). • Cliquez le bouton « Suivant » :

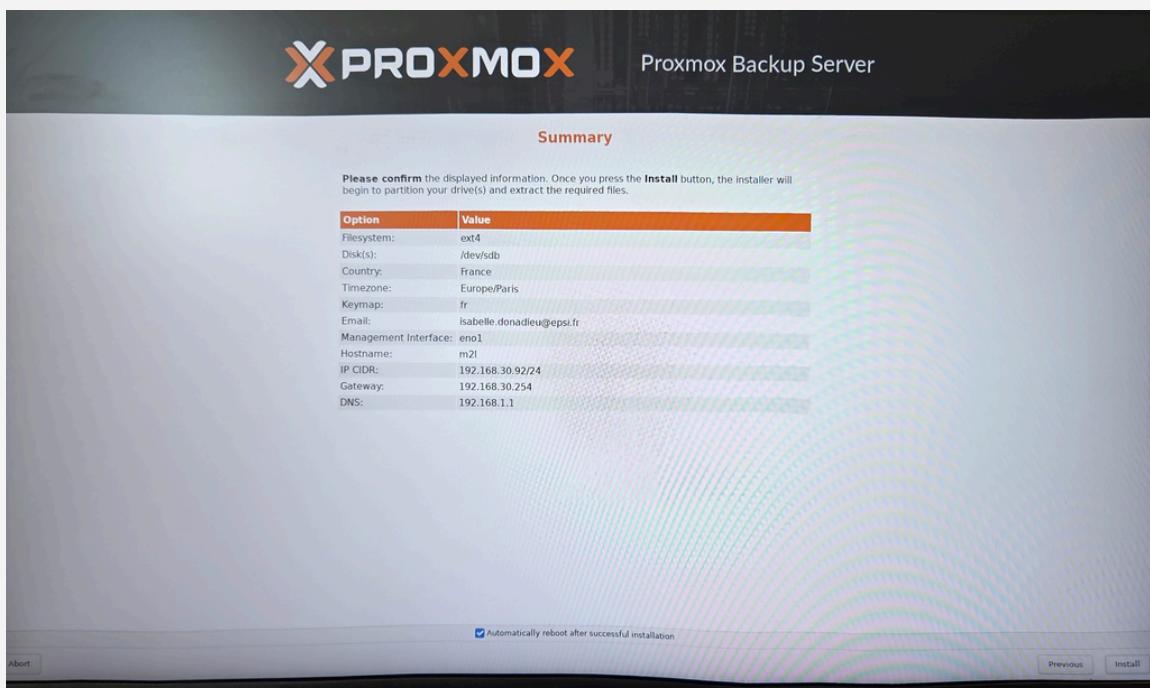


# Installation de Proxmox

- Saisissez, dans la fenêtre ci-dessous, le « Hostname (FQDN) », c'est-à-dire le nom qui sera attribué à votre hyperviseur (ici nous l'avons nommé tout simplement « Proxmox.local »). Les adresses IP sont normalement directement affectées par votre box via le service DHCP mais il est possible de les modifier le cas échéant.
- Cliquez le bouton « Suivant » une fois les paramètres saisis :

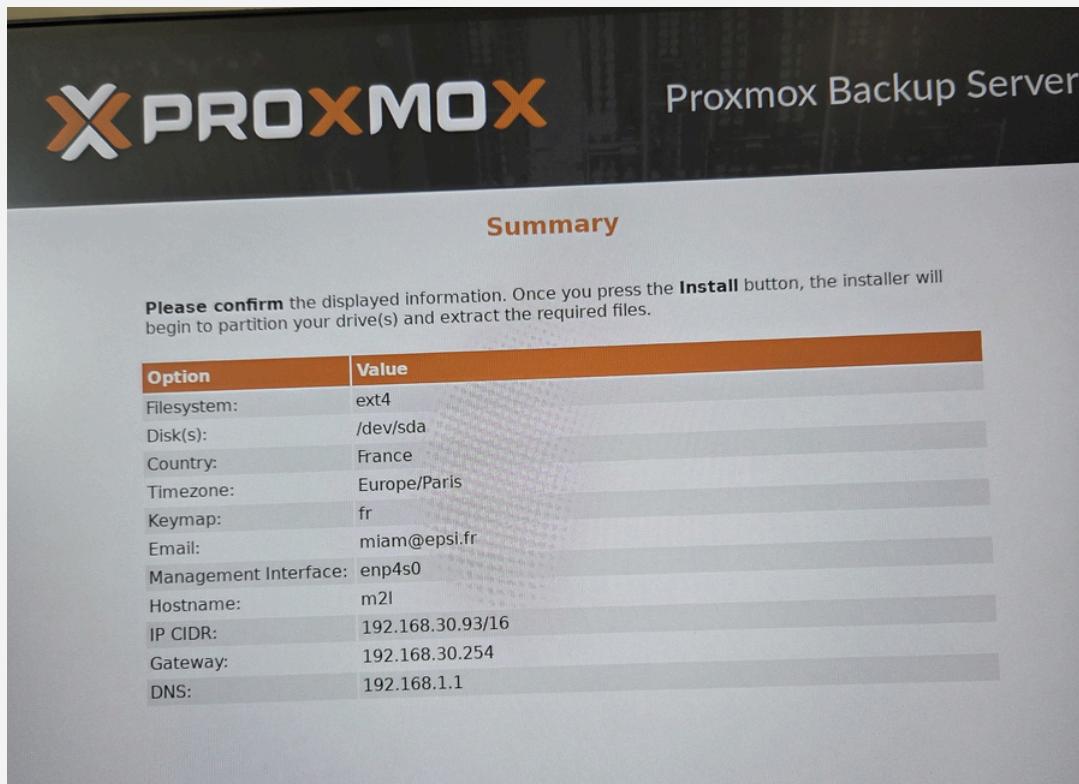


Vérifiez votre configuration et, si tout est correct, cliquez le bouton « Installer » pour lancer l'installation complète de l'hyperviseur Proxmox sur votre machine :

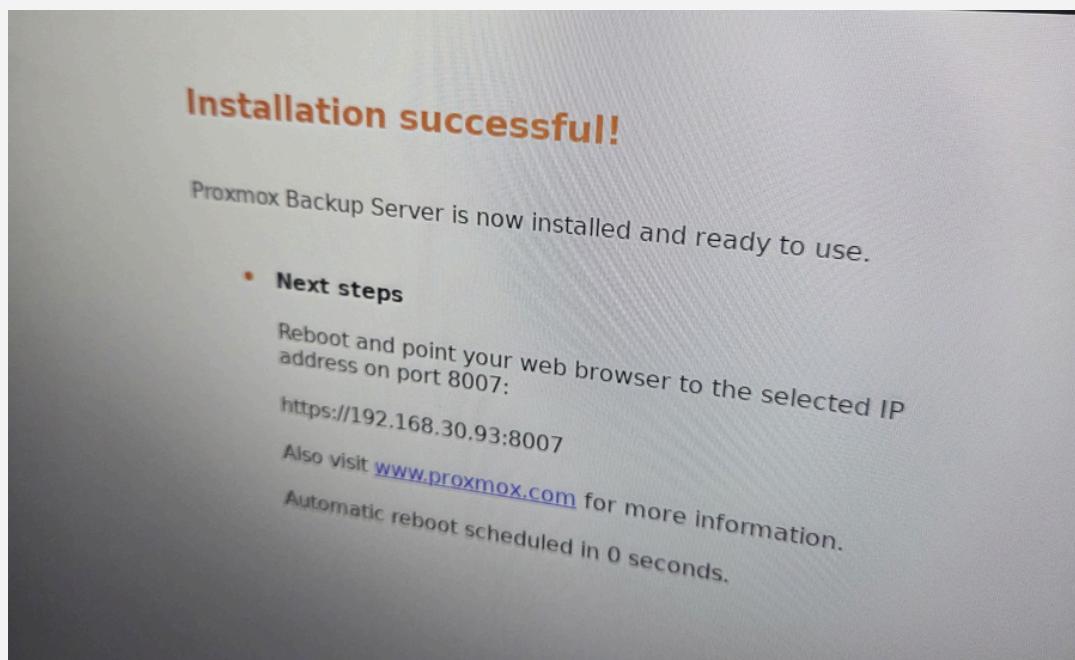


# Installation de Proxmox

Après l'installation, un résumé des informations de Proxmox s'affiche.



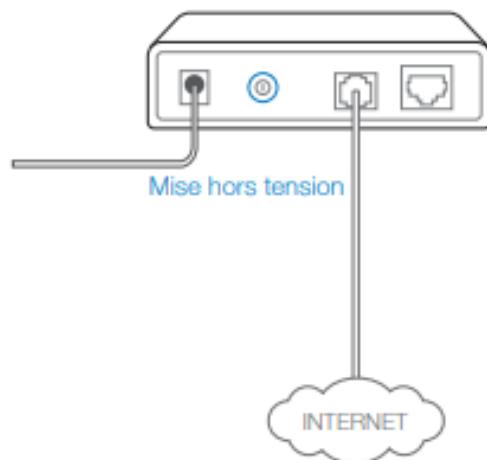
Enfin, une page de confirmation indique que l'installation a été réalisée avec succès et affiche l'adresse IP à utiliser pour accéder à Proxmox.



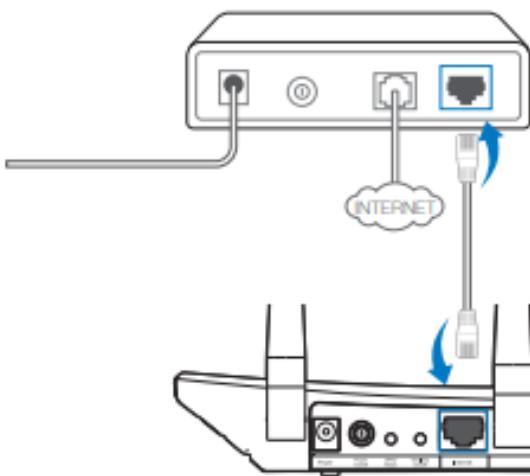
# Connexion à la borne

## 1. Connexion du matériel

- 1 Éteignez le modem et retirez la batterie s'il y en a une.

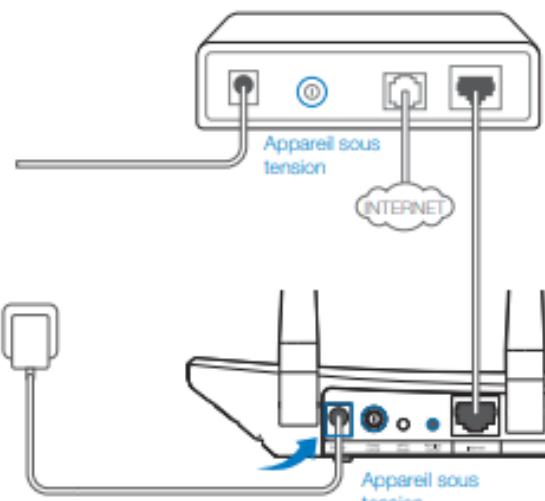


- 2 Raccordez le modem au port Internet de votre routeur à l'aide d'un câble Ethernet.



Remarque : Si votre connexion Internet passe par un câble Ethernet et non par un modem DSL/câblé/Satellite, connectez le

- 3 Allumez le modem, patientez 2 minutes puis allumez le routeur.



- 4 Vérifiez les DEL suivantes pour confirmer que la connexion matérielle fonctionne correctement.



câble Ethernet directement sur le port Internet du routeur.

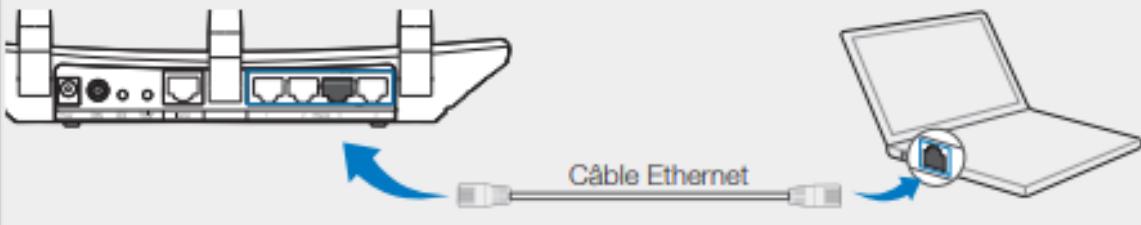


# Connexion à la borne

## 2. Configuration du routeur

- 1 Raccordez votre ordinateur au routeur (connexion filaire ou sans fil).

- Filaire



- Sans fil

Ou  
Activez la connexion sans fil avec le nom du réseau (SSID) et le mot de passe par défaut figurant sur l'étiquette du produit, au dos du routeur.



# Connexion à la borne

2 Ouvrez un navigateur Web sur l'ordinateur et configurez le routeur selon les indications suivantes.

a Saisissez **http://tplinkwifi.net** dans la barre d'adresse.

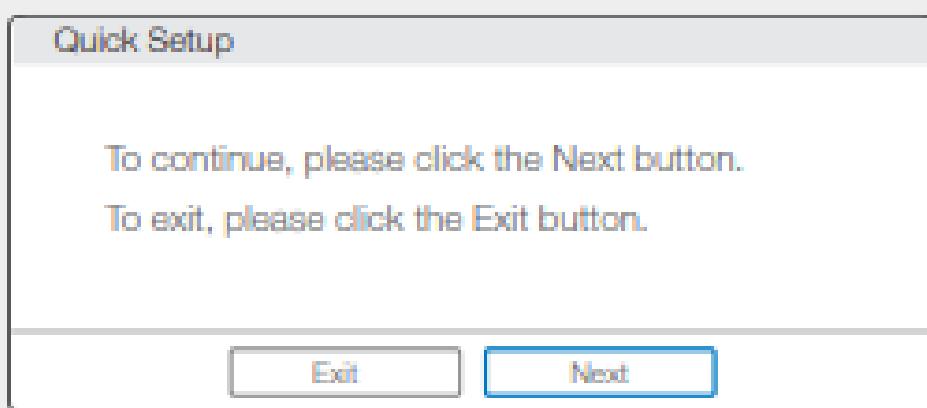
Entrez admin comme identifiant et mot de passe et cliquez sur **Login (Identification)**.

Remarque : Si la fenêtre d'identification n'apparaît pas, reportez-vous à FAQ > Q1.



Copyright © 2014 TP-LINK Technologies Co., Ltd. All rights reserved.

b Cliquez sur **Next (Suivant)** pour poursuivre l'Installation rapide.



# Configuration de la borne

- C Sélectionnez votre type de connexion WAN ou, en cas de doute, cliquez sur **Auto-Detect (DéTECT. auto)**. Cliquez sur **Next (Suivant)** et lisez les instructions pour continuer.

Quick Setup-WAN Connection Type

Auto-Detect  
 Dynamic IP (Most Common Cases)  
 Static IP  
 PPPoE/Russian PPPoE  
 L2TP/Russian L2TP  
 PPTP/Russian PPTP

[Back](#) [Next](#)

- d Vérifiez ou changez les paramètres du réseau sans fil et cliquez sur **Next (Suivant)**.

Remarque : Vous pouvez personnaliser le nom de votre réseau sans fil et votre mot de passe. Dans ce cas, pensez à les noter.

Quick Setup- Wireless

Wireless Network Name:

Wireless Security:  
Wireless Password:

[Back](#) [Next](#)

- e Cliquez sur **Finish (Terminer)** pour achever la procédure.

Quick Setup-Finish

Congratulations!

[Back](#) [Finish](#)

Et c'est parti!

Vos périphériques filaires et sans fil peuvent désormais se connecter à Internet !

# **Portail Captif**

---

# **Explication et Rôle**

Quand on se connecte à un Wi-Fi public, genre dans une école, un hôtel ou un resto, on tombe souvent sur une page qui s'ouvre toute seule avant d'avoir Internet. Cette page, c'est ce qu'on appelle un portail captif.

Son but, c'est pas juste de nous embêter : il sert à vérifier qui se connecte et à protéger le réseau. En gros, tant que t'as pas accepté les conditions ou que tu t'es pas identifié, tu peux pas aller sur Internet.

À quoi ça sert ?

Le portail captif permet de :

- Limiter l'accès au réseau (éviter que tout le monde s'y connecte librement)
- Identifier les utilisateurs, souvent avec un identifiant, un mot de passe ou une adresse mail
- Éviter les abus, genre téléchargements illégaux ou attaques réseau
- Parfois aussi, il sert à collecter des infos pour des raisons légales ou statistiques (toujours avec accord)

EN COURS DE RÉALISATION.

# Conclusion

---

L'implémentation d'un portail captif et de bornes WiFi à la Maison des Ligues de Lorraine (M2L) représente une étape stratégique dans la modernisation de la gestion des accès réseau et de la connectivité des utilisateurs. Avant cette mise en place, la M2L faisait face à une gestion fragmentée et peu sécurisée des connexions WiFi, rendant difficile le contrôle des accès, la gestion des utilisateurs et la sécurisation du réseau. L'absence d'une solution centralisée pour réguler et surveiller les connexions compliquait également l'administration du réseau et pouvait exposer l'infrastructure à des risques de sécurité.

En optant pour un portail captif couplé à un déploiement de bornes WiFi, la M2L a pu centraliser et sécuriser l'accès à son réseau sans fil. Le portail captif permet désormais d'authentifier les utilisateurs avant qu'ils n'accèdent à Internet, en imposant une identification par mot de passe, adresse e-mail, ou autre méthode d'authentification définie. Cette solution offre un contrôle accru sur les connexions, permettant d'appliquer des règles d'accès adaptées aux différents profils d'utilisateurs (personnel, visiteurs, ligues sportives) et de limiter les abus d'utilisation de la bande passante.

Le déploiement des bornes WiFi a permis d'améliorer la couverture réseau dans l'ensemble des locaux de la M2L, garantissant une connexion stable et performante pour les employés, les partenaires et les visiteurs. Grâce à une gestion centralisée des points d'accès, l'administration peut désormais surveiller en temps réel l'état du réseau, détecter d'éventuelles anomalies et optimiser la répartition du signal pour assurer une qualité de service homogène sur l'ensemble du site.

La mise en place de cette solution a également renforcé la sécurité du réseau en séparant les flux de trafic selon les profils utilisateurs via des VLANs dédiés. Cela permet d'éviter les intrusions et de limiter les risques d'attaques en isolant les connexions des invités du réseau interne. De plus, les logs des connexions sont conservés conformément aux réglementations en vigueur, offrant ainsi une traçabilité en cas d'incident de sécurité.

En somme, l'implémentation d'un portail captif et de bornes WiFi à la M2L a permis de moderniser la gestion des accès réseau, d'optimiser la qualité de la connexion et d'améliorer la sécurité globale du système. Cette infrastructure offre une meilleure expérience aux utilisateurs tout en facilitant l'administration et le contrôle du réseau. Ce projet illustre l'importance d'adopter des solutions de gestion centralisée pour les infrastructures réseau, en particulier dans des environnements où la connectivité joue un rôle clé dans le bon déroulement des activités. Grâce à cette modernisation, la M2L est désormais mieux équipée pour répondre aux besoins croissants des ligues sportives et de ses partenaires en matière de connectivité, tout en garantissant un environnement réseau sécurisé et performant. Cette solution pourrait également être adoptée par d'autres institutions cherchant à améliorer la gestion et la sécurité de leur réseau WiFi.

# 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 : BANANE Mohamed		N° candidat : 02047225428
<input checked="" type="checkbox"/> Épreuve ponctuelle <input type="checkbox"/> Contrôle en cours de formation		Date :
<b>Organisation support de la réalisation professionnelle</b> 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 réseau sans fil sécurisé pour ses utilisateurs et ses invités		
<b>Intitulé de la réalisation professionnelle</b> Installation et configuration des bornes WIFI + portail captif		
Période de réalisation : 04/11/2024 - 20/12/2024	Lieu : EPSI MONTPELLIER ▾	
Modalité :	<input type="checkbox"/> Seul	<input checked="" type="checkbox"/> En équipe
cl		
<b>Compétences travaillées</b> <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		
<b>Conditions de réalisation<sup>1</sup> (ressources fournies, résultats attendus)</b>		
Ressources fournies :	Résultats attendus :	
<ul style="list-style-type: none"><li>• Cahier des charges M2L</li><li>• Serveur physique</li><li>• Proxmox VE 8.2</li><li>• Bornes WI-FI TP-LINK (AC1350)</li><li>• Serveur Web (Apache)</li></ul>	<ul style="list-style-type: none"><li>• Gestion des réseaux WiFi</li><li>• Sécurisation du réseau Wi-Fi</li><li>• Gestion des accès et des connexions</li></ul>	
<b>Description des ressources documentaires, matérielles et logicielles utilisées<sup>2</sup></b>		
<ul style="list-style-type: none"><li>• Schéma réseau M2L</li><li>• Documentation d'installation et configuration d'une borne wifi</li><li>• Documentation d'installation et configuration d'un portail captif</li><li>• Documentation d'installation et configuration d'un client Windows/Linux</li></ul>		
<b>Modalités d'accès aux productions<sup>3</sup> et à leur documentation</b>		
Lien de production : <a href="https://thegreatestbanana.github.io/PortFolioBTS/mohamedbanana.com/index.html">https://thegreatestbanana.github.io/PortFolioBTS/mohamedbanana.com/index.html</a>		
Documentations techniques <a href="https://lnsh.xyz/6044a7">lnsh.xyz/6044a7</a>		
Lien de documentations :		
<ul style="list-style-type: none"><li>• Wi-Fi : <a href="https://lnsh.xyz/159fa7">lnsh.xyz/159fa7</a></li><li>• Proxmox : <a href="https://lnsh.xyz/c5f533">lnsh.xyz/c5f533</a></li><li>• VLAN : <a href="https://lnsh.xyz/613101">lnsh.xyz/613101</a></li></ul>		

