

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 :

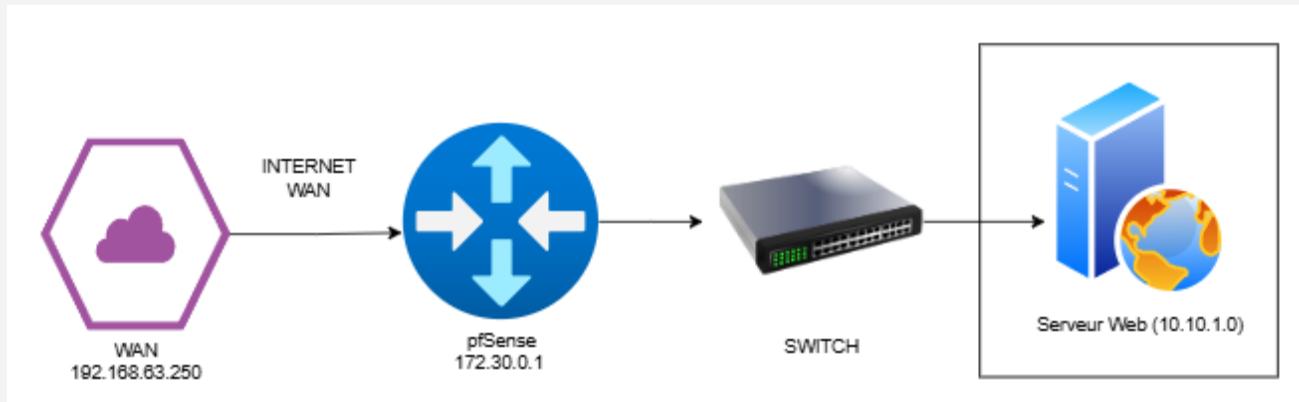
- La M2L souhaite moderniser son infrastructure WiFi en :
- Offrant un accès WiFi sécurisé et centralisé aux ligues et visiteurs.
- Contrôlant et authentifiant les utilisateurs via un portail captif.
- Optimisant la gestion des ressources réseau (bande passante, adresses IP, restrictions d'usage).

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.

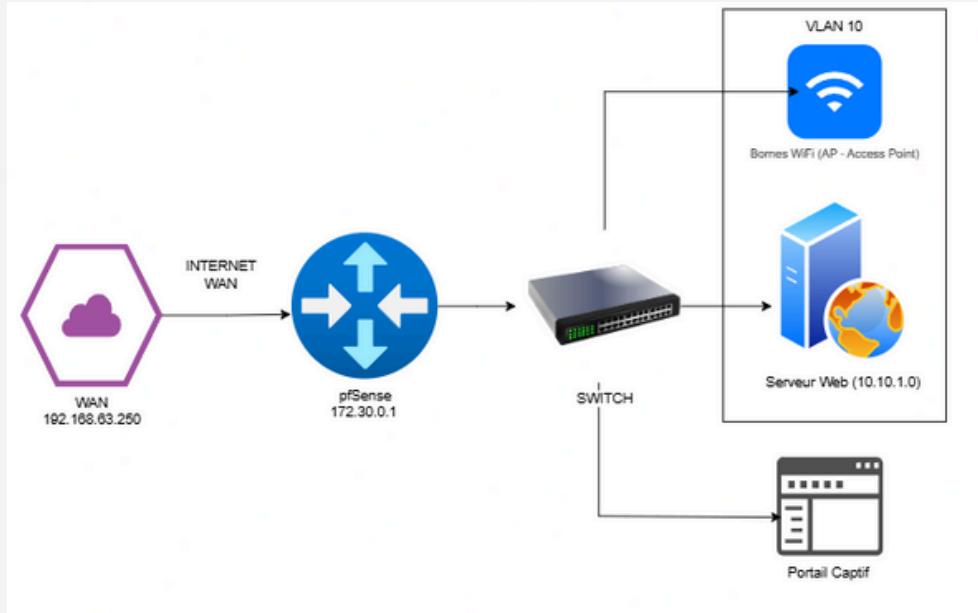
4. Expérience utilisateur améliorée

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 :

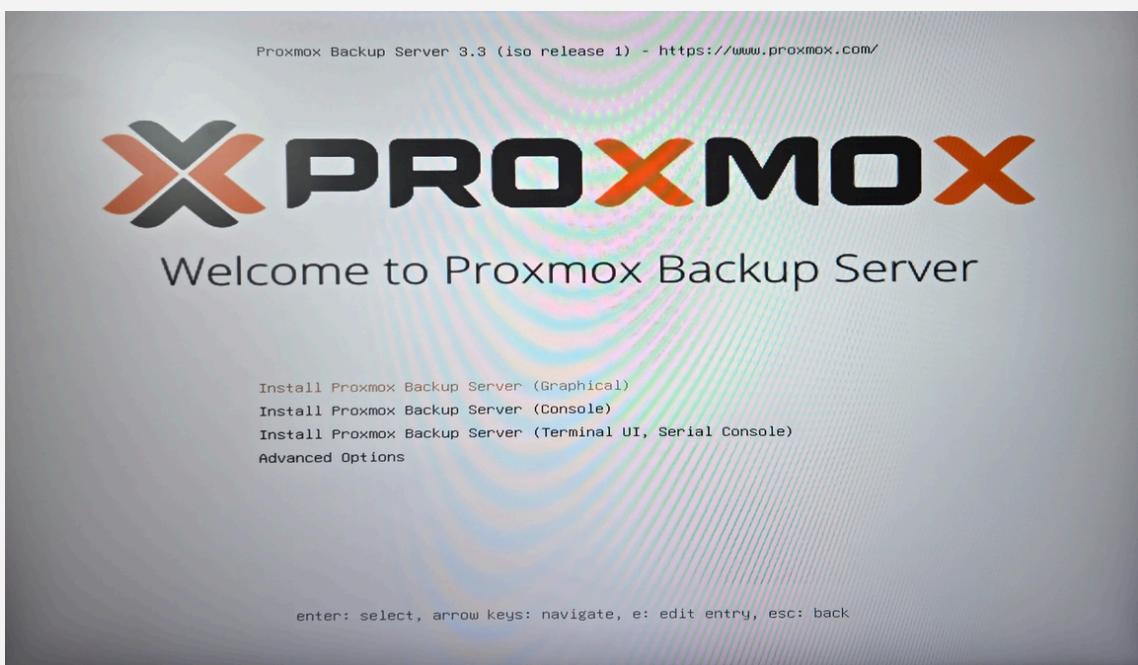
- **WAN (192.168.63.250)** : L'interface WAN reste inchangée, permettant toujours la connexion à Internet.
- **PfSense (172.30.0.1)** : Le pare-feu PfSense continue de gérer les règles de sécurité et le filtrage, mais maintenant avec une meilleure gestion de la communication vers le portail captif.
- **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.

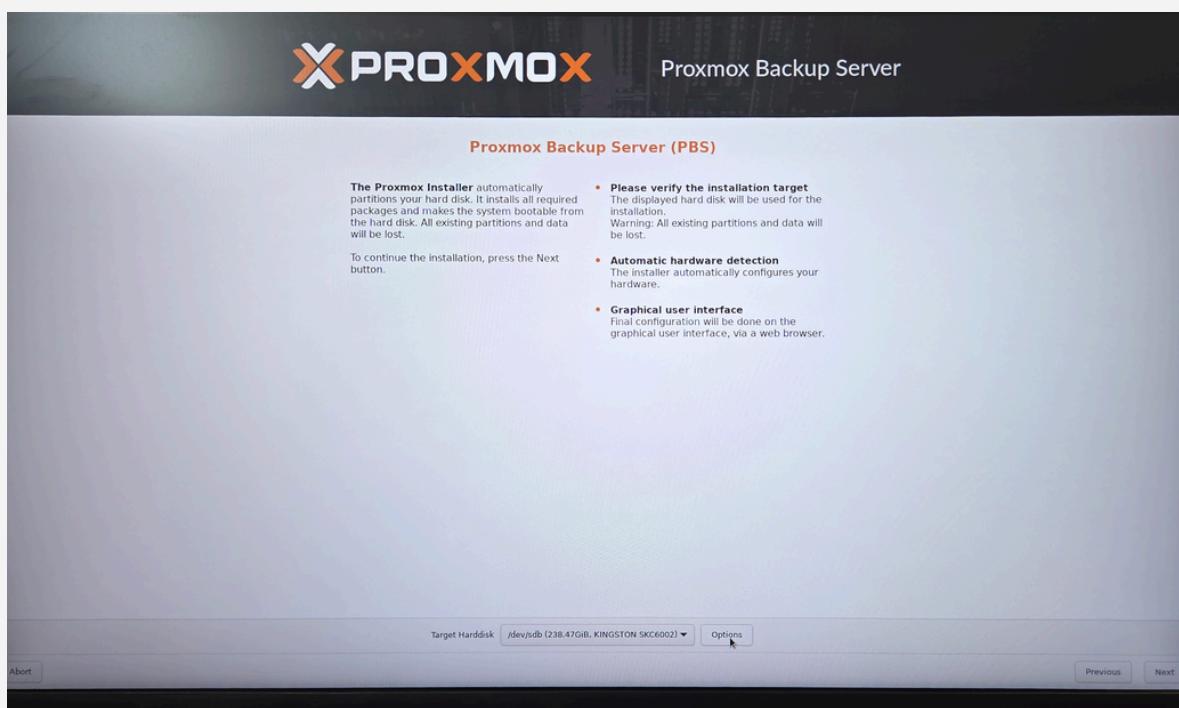


Installation de Proxmox

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 :

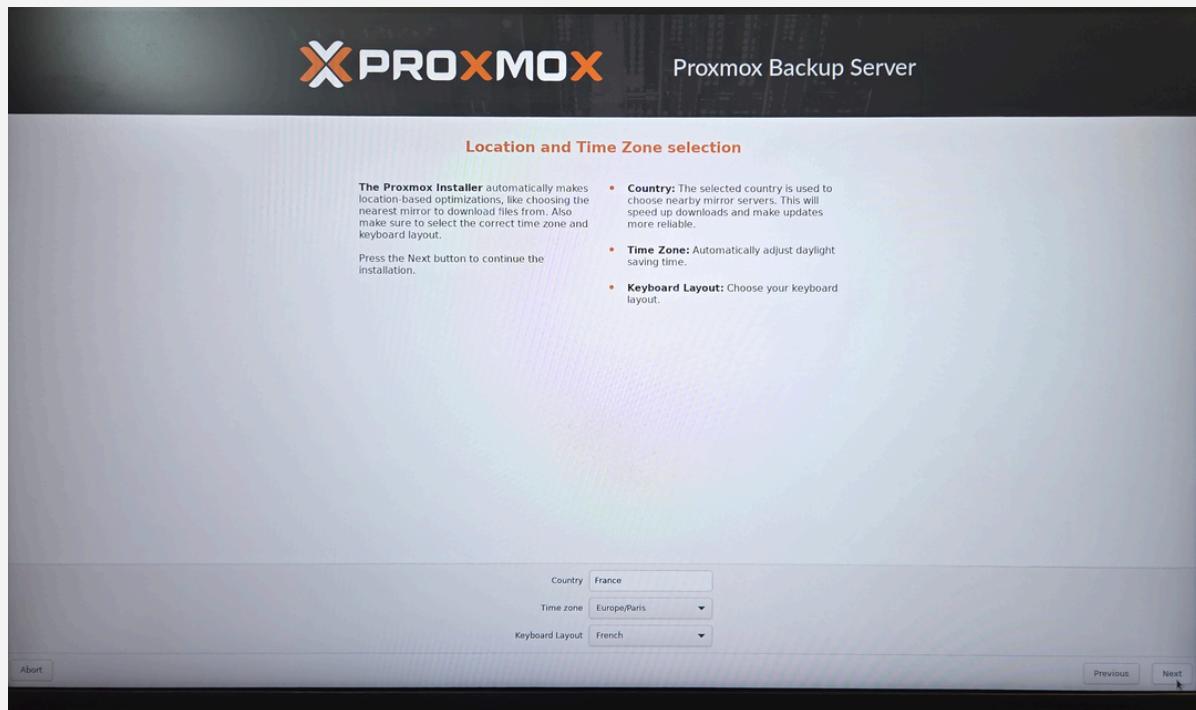


Sélectionnez, dans la fenêtre suivante, le disque sur lequel le système sera installé et cliquez le bouton « Suivant » :

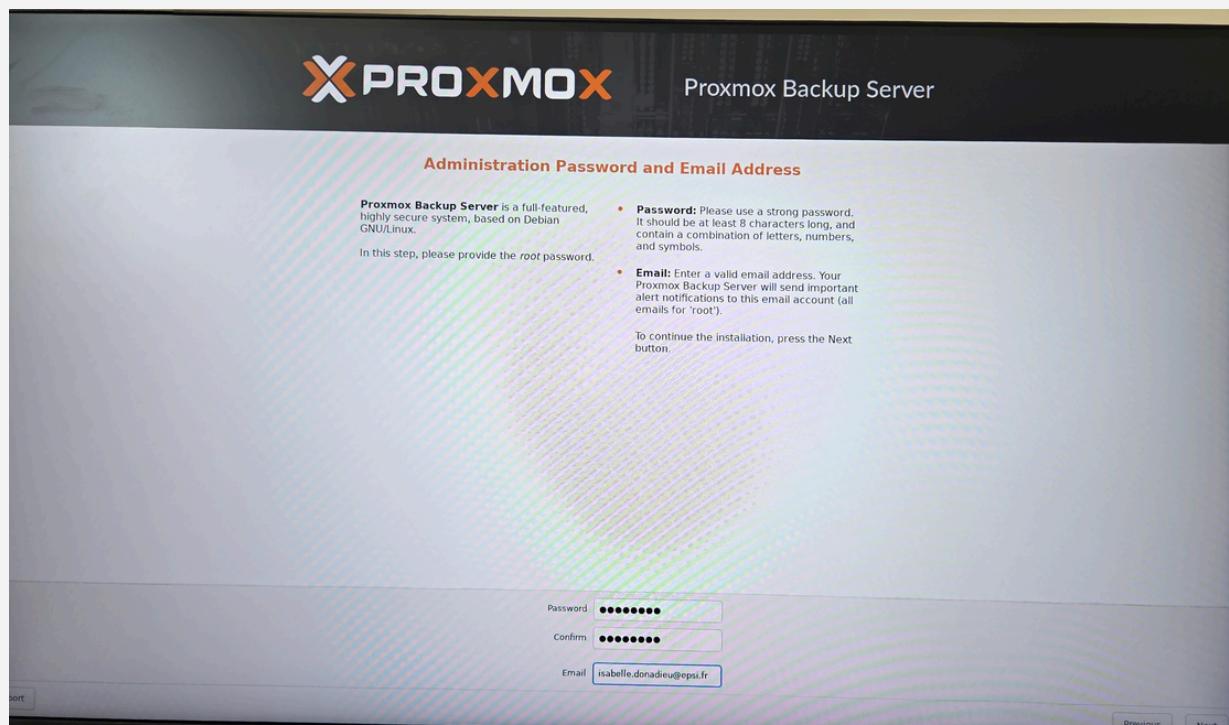


Installation de Proxmox

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

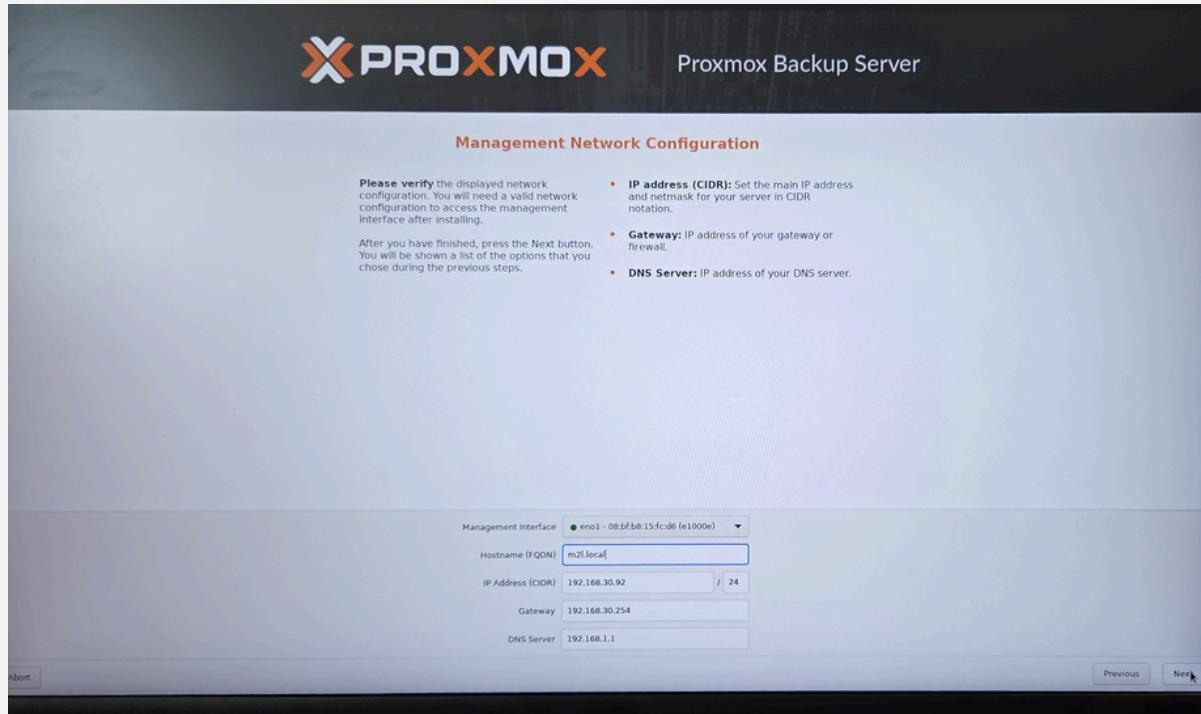


Saisissez le mot de passe qui sera attribué au compte « root » (super utilisateur) de Proxmox et indiquez un compte mail valide (qui vous permettra de recevoir différentes notifications en lien avec votre serveur Proxmox). • Cliquez le bouton « Suivant » :

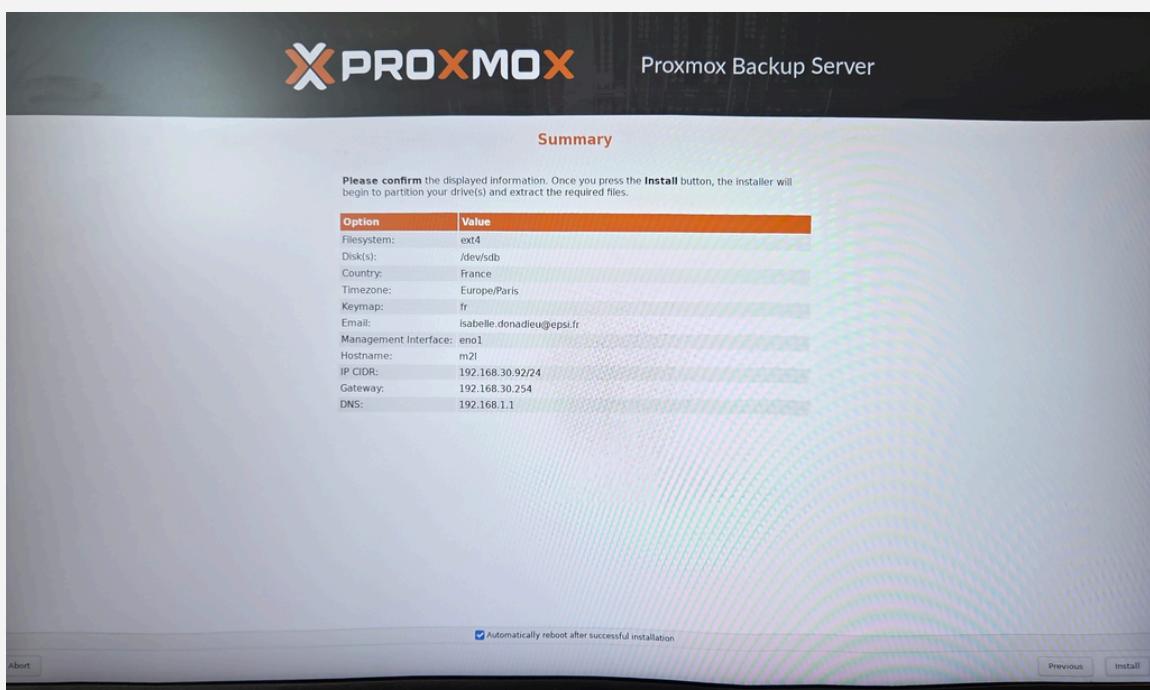


Installation de Proxmox

- 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 :

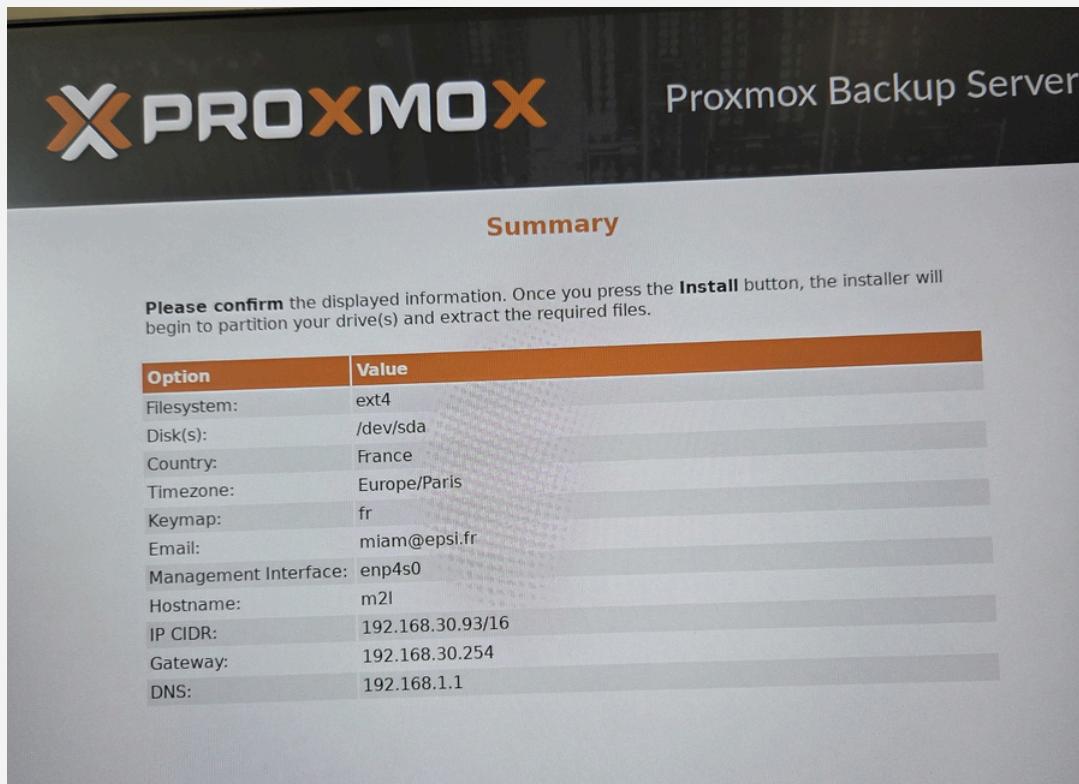


Vérifiez votre configuration et, si tout est correct, cliquez le bouton « Installer » pour lancer l'installation complète de l'hyperviseur Proxmox sur votre machine :

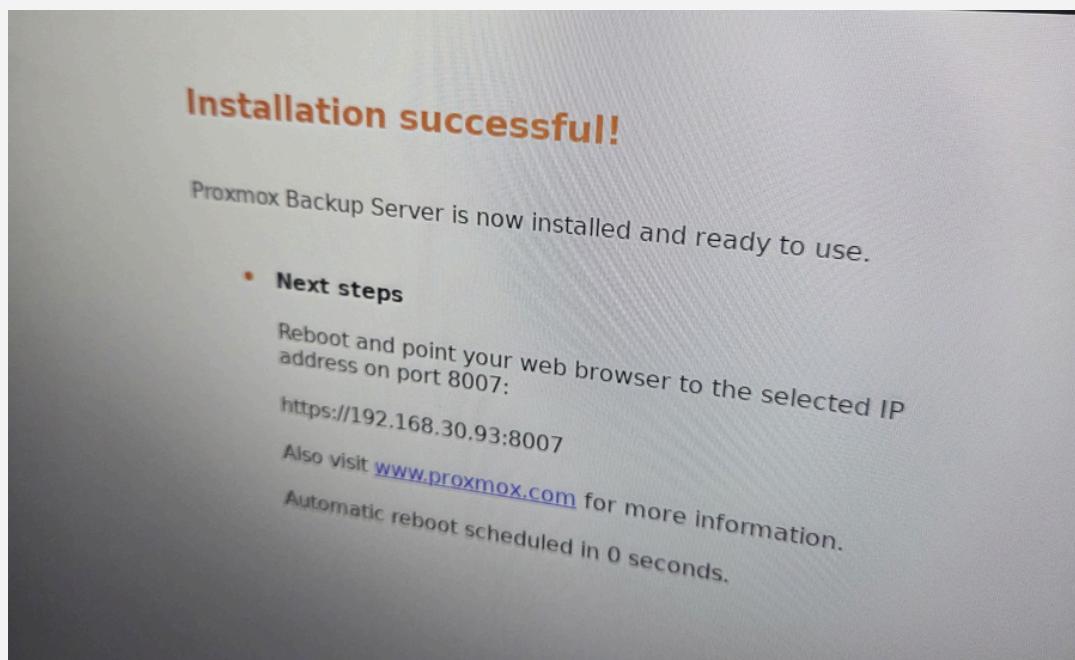


Installation de Proxmox

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



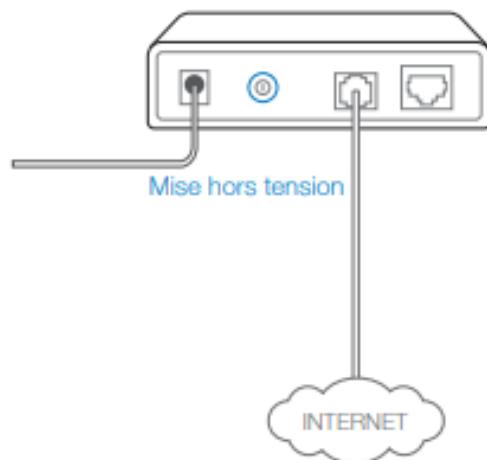
Enfin, une page de confirmation indique que l'installation a été réalisée avec succès et affiche l'adresse IP à utiliser pour accéder à Proxmox.



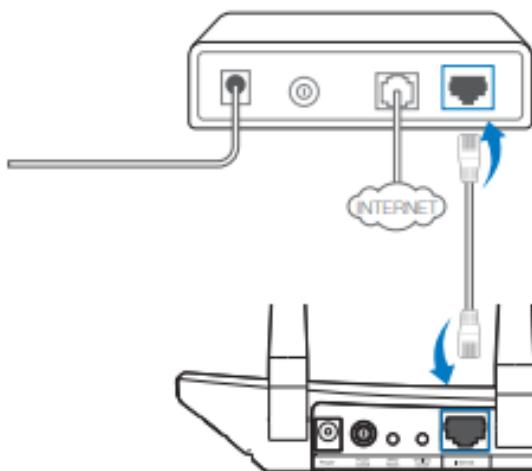
Connexion à la borne

1. Connexion du matériel

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



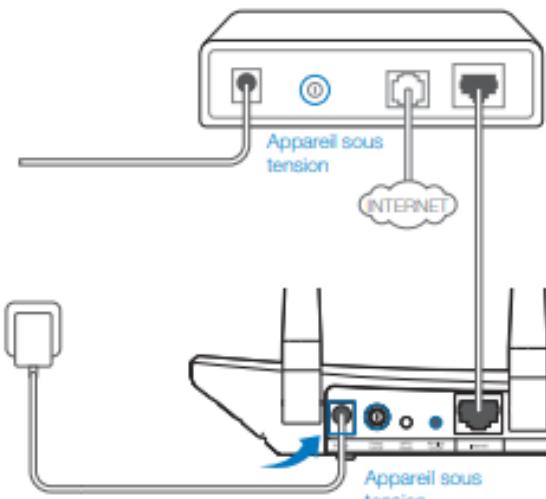
- 2 Raccordez le modem au port Internet de votre routeur à l'aide d'un câble Ethernet.



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

Suivre les étapes pour pouvoir accéder à l'interface de la borne Wi-fi.

- 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.

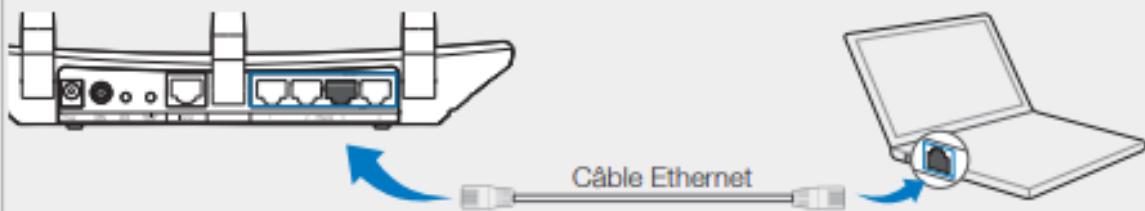


Connexion à la borne

2. Configuration du routeur

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

- Filaire



Ici, on va suivre la façon filaire car on accès à la borne wifi en physique.

- 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.



Mais si on ne peut pas se connecter de manière physique alors on peut suivre l'étape sans fil.

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.

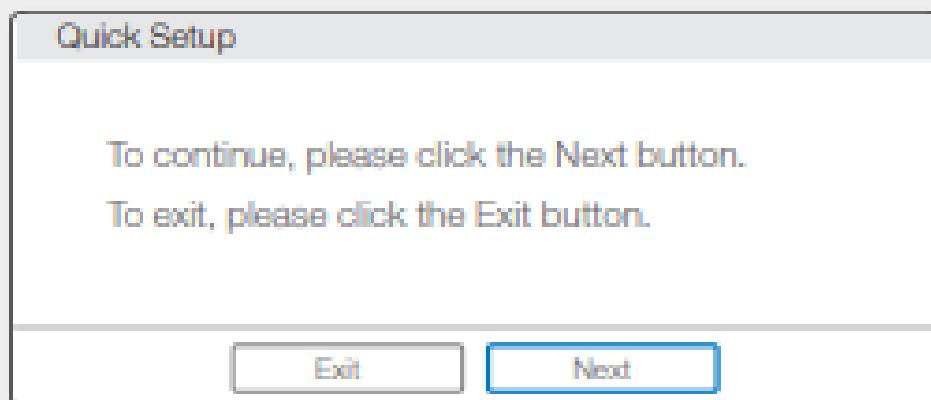
Entrez admin comme identifiant et mot de passe et cliquez sur **Login (Identification)**.

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



On rentre le lien à la main et une interface web s'affiche le login et le mot de passe sont à l'arrière de la borne généralement admin/admin.

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



On peut ensuite commencer la configuration de la borne wifi et suivre les étapes suivantes.

Portail Captif

Explication et Rôle

Pourquoi utiliser un portail captif ?

Lorsque l'on se connecte à un réseau Wi-Fi public — comme dans une école, un hôtel, un restaurant ou dans une structure comme la Maison des Ligues de Lorraine (M2L) — il est fréquent d'être redirigé automatiquement vers une page web avant de pouvoir accéder à Internet. Cette page s'appelle un portail captif.

Le portail captif a pour fonction principale de sécuriser le réseau en contrôlant l'accès des utilisateurs. Il empêche toute navigation tant que l'utilisateur n'a pas accepté les conditions d'utilisation ou ne s'est pas authentifié. Il s'agit donc d'une première barrière de protection avant l'accès à Internet.

À quoi sert un portail captif ?

Un portail captif permet de :

- Limiter l'accès au réseau : seules les personnes autorisées peuvent se connecter, évitant ainsi l'accès libre à toute personne à proximité.
- Identifier les utilisateurs : via un mot de passe, un identifiant, une adresse e-mail, ou un compte temporaire.
- Prévenir les abus : comme les téléchargements illégaux, les attaques réseau ou l'utilisation excessive de la bande passante.
- Répondre aux obligations légales : certaines réglementations exigent la traçabilité des connexions à Internet.
- Afficher des messages informatifs ou des conditions d'utilisation avant toute connexion.

Intérêt du portail captif dans le contexte de la M2L

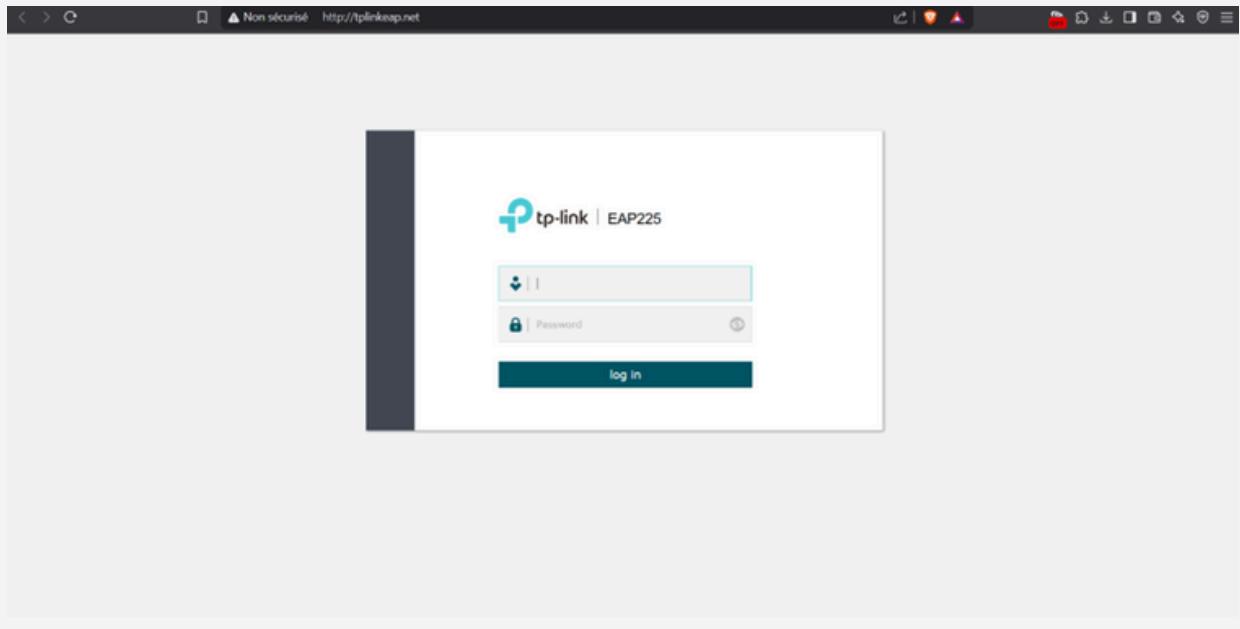
La Maison des Ligues de Lorraine est un établissement accueillant plusieurs ligues sportives et structures associées. Elle a pour mission d'offrir un environnement stable, sécurisé et adapté à ses utilisateurs, qu'ils soient permanents ou temporaires.

Dans cette optique, l'utilisation d'un portail captif permet à la M2L de :

- Sécuriser l'accès au réseau Wi-Fi en forçant l'authentification ou l'acceptation des règles d'usage.
- Mettre en place une différenciation claire entre les utilisateurs (ligues, visiteurs, personnel) grâce à plusieurs réseaux sans fil configurés avec des droits spécifiques.
- Contrôler l'utilisation du réseau : gestion de la bande passante, attribution dynamique des adresses IP, filtrage des contenus, et restrictions d'usage.
- Garantir une traçabilité des connexions, en accord avec les exigences réglementaires.
- Faciliter l'administration du réseau à travers une interface centralisée pour la gestion des accès et des équipements.

Portail Captif

Explication et Rôle



Cette capture montre l'interface d'administration de la borne TP-Link, accessible via un navigateur web. Par défaut, l'identifiant et le mot de passe sont tous deux définis sur admin. Cette étape est nécessaire pour accéder aux paramètres de configuration de la borne Wi-Fi.

Set up a new account

New Username: admin

New Password: Low Middle High

Confirm Password: X

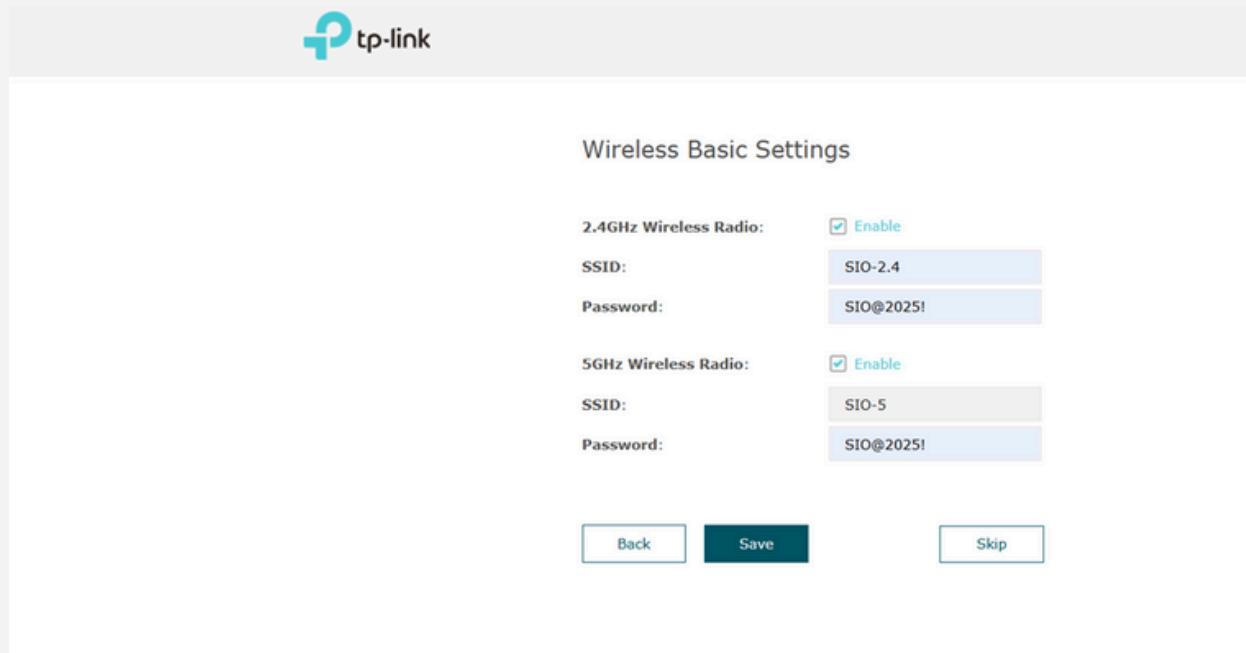
Next

Ici, l'utilisateur modifie le nom d'utilisateur et le mot de passe par défaut afin de sécuriser l'accès à l'interface d'administration de la borne. Cette étape est cruciale pour empêcher tout accès non autorisé au système.

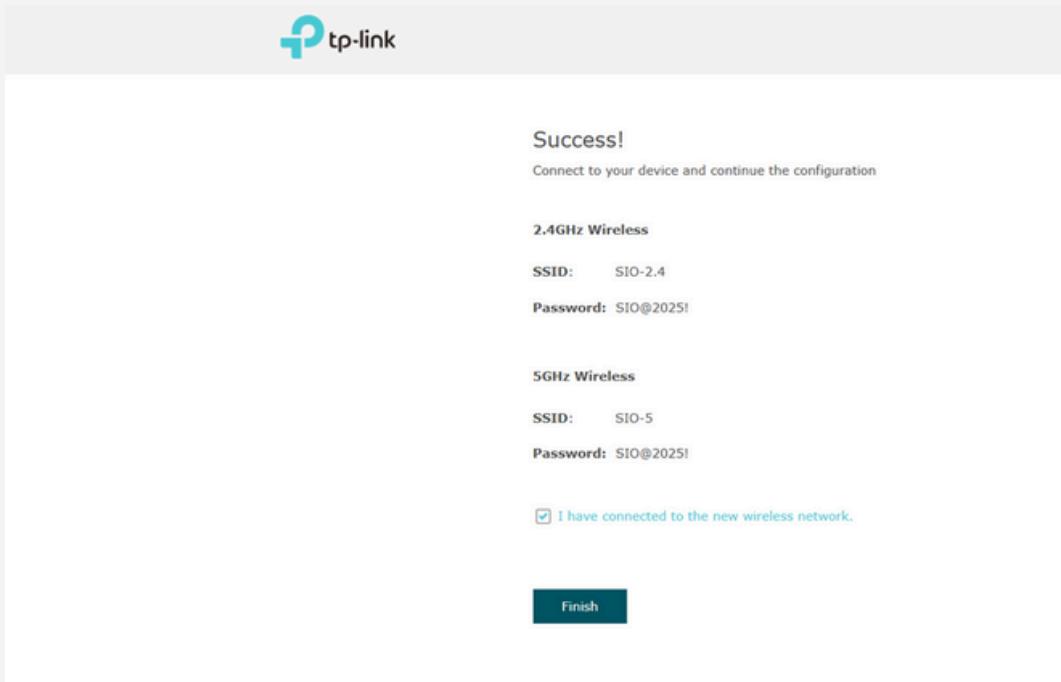


Portail Captif

Explication et Rôle



Cette capture illustre la modification du nom des réseaux Wi-Fi (SSID) et de leurs mots de passe. Deux réseaux distincts sont configurés, chacun avec son propre nom et mot de passe pour mieux organiser les connexions (par exemple : personnel et invité).

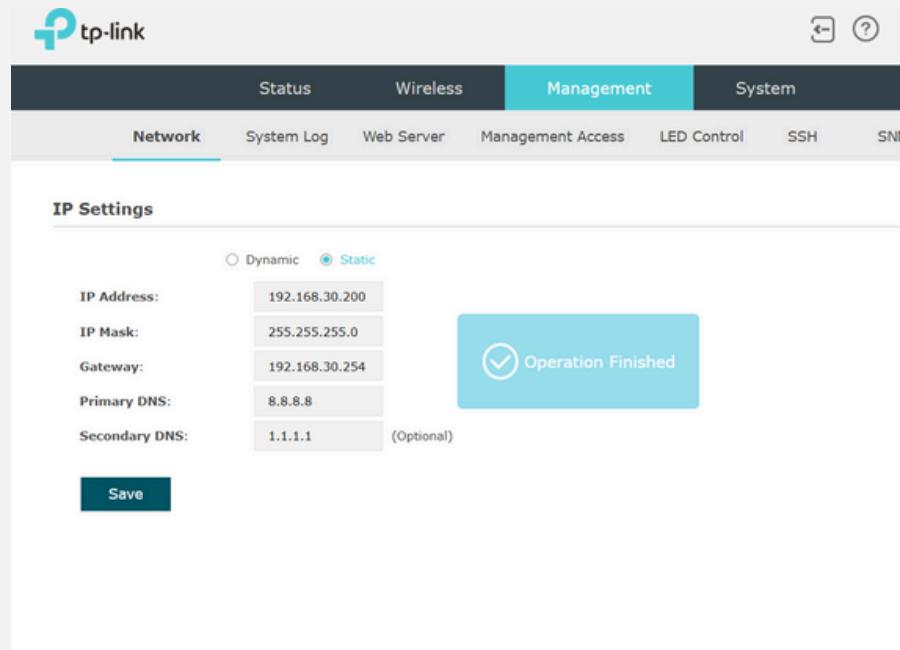


Un résumé clair des nouveaux identifiants et mots de passe est présenté. Cette étape permet de vérifier que les informations de connexion ont bien été enregistrées et seront utilisées pour se connecter aux réseaux créés.



Portail Captif

Explication et Rôle



Dans le menu Management > Network, la borne est configurée avec une adresse IP statique. Cela permet de la localiser facilement sur le réseau et d'assurer une meilleure stabilité. Cette étape inclut également la création de l'utilisateur administrateur.

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network
--	--	--	--	--	--

SSID: SIO-VLAN10
SSID Broadcast: Enable
Security Mode: WPA-Personal
Version: WPA2-PSK
Encryption: Auto TKIP AES
Wireless Password: SIO@2025|
Group Key Update Period: 0 seconds (30-8640000. 0 means no update.)
Guest Network: Enable [i](#)
Rate Limit: Enable

OK **Cancel**

Cette capture marque le début de la mise en place du portail captif. Ce système permet de contrôler l'accès à Internet en forçant les utilisateurs à passer par une page d'authentification ou d'acceptation des conditions avant de naviguer.



Portail Captif

Explication et Rôle

The screenshot shows the TP-Link web interface with the following navigation bar:

- Status
- Wireless
- VLAN** (highlighted)
- Management
- System

Below the navigation bar, there are sub-links:

- Wireless Settings
- Portal
- VLAN** (highlighted)
- MAC Filtering
- Scheduler
- Band Steering
- QoS
- Rogue AP Detection

The main content area is titled "VLAN ID" and contains a table with the following data:

ID	SSID Name	Band	VLAN	VLAN ID
1	SIO-VLAN10	2.4GHz	Enable	10
2	SIO-VLAN20	2.4GHz	Enable	20
3	SIO-VLAN30	2.4GHz	Enable	30
4	SIO-VLAN50	2.4GHz	Enable	50
5	SIO-VLAN99	2.4GHz	Enable	99

At the bottom of the table, there is a "Save" button.

Première étape

The screenshot shows the TP-Link web interface with the following navigation bar:

- Status
- Wireless
- VLAN**
- Management
- System

Below the navigation bar, there are sub-links:

- Wireless Settings
- Portal
- VLAN**
- MAC Filtering
- Scheduler
- Band Steering
- QoS
- Rogue AP Detection

The main content area is titled "2.4GHz SSIDs" and contains a table with the following data:

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
1	SIO-VLAN10	10	Enable	WPA-Personal	Disable	<input checked="" type="checkbox"/> Delete
2	SIO-VLAN20	20	Enable	WPA-Personal	Disable	<input checked="" type="checkbox"/> Delete
3	SIO-VLAN30	30	Enable	WPA-Personal	Disable	<input checked="" type="checkbox"/> Delete
4	SIO-VLAN50	50	Enable	WPA-Personal	Disable	<input checked="" type="checkbox"/> Delete
5	SIO-VLAN99	99	Enable	WPA-Personal	Disable	<input checked="" type="checkbox"/> Delete

Ici, les conditions d'utilisation du réseau sont définies dans le portail captif. Elles précisent les règles à respecter pour bénéficier de la connexion Wi-Fi et doivent être acceptées par l'utilisateur avant tout accès à Internet.



Portail Captif

Explication et Rôle

Portal Configuration

Authentication Type:	External Radius Server
Radius Server IP:	192.168.1.103
Port:	1812
Radius Password:	testing123
Authentication Timeout:	1 Hours
	0 D 0 H 10 M
Redirect:	<input checked="" type="checkbox"/> Enable
Redirect URL:	http://www.tp-link.com

Première étape

The screenshot shows the TP-Link web interface with the following navigation bar:

- Status
- Wireless
- Management
- System

The "Portal" tab is selected. The main section is titled "Portal Configuration" and contains the following fields:

- SSID: SIO-VLAN30
- Authentication Type: Local Password
- Password: SIO@2025!
- Authentication Timeout: 1 Hour
- Redirect: Enable
- Redirect URL: [http://www.tp-link.com](#)
- Portal Customization: Local Web Portal

A preview window shows a login page with the following content:

Portal Wi-Fi
EPSI SIO

Password:

Term of Use:

3. Security
- The Service is provided over a public network. You are responsible for ensuring the security of your device and personal information.

I accept the Term of Use

Login

At the bottom left is a "Save" button.

Ici, les conditions d'utilisation du réseau sont définies dans le portail captif. Elles précisent les règles à respecter pour bénéficier de la connexion Wi-Fi et doivent être acceptées par l'utilisateur avant tout accès à Internet.



Portail Captif

Explication et Rôle

**Portal Wi-Fi
EPSI SIO**

Password:

Term of Use:

Terms of Use – Wi-Fi Portal

Effective Date: 2025

By accessing and using this Wi-Fi service (the "Service"), you agree to the following terms and conditions:

1. Access and Availability

- The Service is provided for your personal and temporary use.
- Access is subject to availability and may be suspended, interrupted, or limited at any time without notice.

2. User Responsibilities

- You agree not to use the Service for unlawful, harmful, fraudulent, or malicious purposes.
- You must not attempt to access restricted areas, spread viruses, or engage in any activity that may damage or impair the network.

3. Security

- The Service is provided over a public network. You are responsible for ensuring the security of your device and personal information.

I accept the Term of Use

log in

Désormais, lorsqu'un utilisateur se connecte au réseau Wi-Fi, une page de redirection s'affiche automatiquement. Il doit lire et accepter les termes d'utilisation pour accéder à Internet. Cela confirme que le portail captif est actif et fonctionnel.

Portal Login Success!

L'accès au Wi-Fi nécessite désormais une double validation : la saisie du mot de passe du réseau, suivie de l'acceptation des conditions d'utilisation via le portail captif.



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 :
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 réseau sans fil sécurisé pour ses utilisateurs et ses invités		
Intitulé de la réalisation professionnelle 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		c
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 réalisation¹ (ressources fournies, résultats attendus)		
Ressources fournies :	Résultats attendus :	
<ul style="list-style-type: none">• Cahier des charges M2L• Serveur physique• Proxmox VE 8.2• Bornes Wi-Fi TP-LINK (AC1350)• Serveur Web (Apache)	<ul style="list-style-type: none">• Gestion des réseaux WiFi• Sécurisation du réseau Wi-Fi• Gestion des accès et des connexions	
Description des ressources documentaires, matérielles et logicielles utilisées²		
<ul style="list-style-type: none">• Schéma réseau M2L• Documentation d'installation et configuration d'une borne wifi• Documentation d'installation et configuration d'un portail captif• Documentation d'installation et configuration d'un client Windows/Linux		
Modalités d'accès aux productions³ et à leur documentation		
Lien de production : https://thegreatestbanana.github.io/PortFolioBTS/mohamedbanana.com/index.html		
Documentations techniques Insh.xyz/6044a7		
Lien de documentations :		
<ul style="list-style-type: none">• Wi-Fi : Insh.xyz/159fa7• Proxmox : Insh.xyz/c5f533• VLAN : Insh.xyz/613101		

