BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-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 : 2**
Nom, prénom : HOUPIN Alicia	**N° candidat : 02543699940**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 30 / 04 / 2026

Organisation support de la réalisation professionnelle
Oasis, société parisienne spécialisée dans les voyages personnalisés.

La réalisation s'inscrit dans le projet de déploiement d'une infrastructure Wi-Fi professionnelle segmentée et sécurisée pour les collaborateurs et les invités à la suite de l'ouverture de l'agence à Marseille

Intitulé de la réalisation professionnelle
Mise en place d'une infrastructure Wi-Fi professionnelle au sein de l'agence de Marseille

Période de réalisation : 02/2026 – 04/2026 **Lieu :** Fab Academy La Roche-sur-Yon

Modalité : ☒ **Seul(e)** ☐ **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)

- Les ressources fournies :
  Contexte professionnel de l'agence de Marseille , topologie réseau cible , plan d'adressage , un contrôleur UniFi 10.1.85 hébergé sur une VM Windows server, une borne Ubiquiti UAP-AC-Lite, un switch manageable Cisco 1000, un firewall Stormshield,SN210, un serveur DHCP centralisé sur une VM Windows server et accès au contrôleur UniFi via une interface Web centralisée
- Les ressources attendues :
  Mise en place d'un Wi-Fi professionnel segmenté (Employés / Invités). Sécurisation des accès. Mise en œuvre d'un portail captif pour les invités

[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.

Description des ressources documentaires, matérielles et logicielles utilisées[2]

- Ressources documentaires :
  Contexte Oasis, topologie réseau de l'agence de Marseille , Documentation Ubiquiti , Documentation Stormshield , plan d'adressage IP et segmentation VLAN (110/130/140)
- Ressources matérielles :
- Borne Wi-Fi Ubiquiti UAP-AC-Lite , Switch manageable Cisco 1000 , Firewall Stormshield SN210 , VM Windows Server 2022 Datacenter pour héberger le contrôleur , câbles RJ45 , infrastructure VLANs 130/140 , Serveur DHCP Windows Server (site de Marseille), PC jury et téléphone portable (test)
- Ressources logicielles :
  Proxmox VE pour l'hébergement des machines virtuelles, Windows Server 2022 Datacenter pour héberger le contrôleur , UniFi Network Controller 10.1.85 , Visual C++ Redistributable (VC_redist.x64) et un navigateur web pour l'administration.

Modalités d'accès aux productions[3] et à leur documentation[4]

- Accès aux productions
  Un PC de démonstration est mis à disposition lors de l'épreuve : compte « jury01 » et mot de passe « LDLrcfgFp725LXfGWLU »
  Serveur accessible depuis le BASTION (connexion RDP : 192.168.10.7), la connexion à tous les serveurs se fait uniquement avec les comptes « administrateur » et « root » renseigné dans le KEEPASS.

- Accès à la documentation
  L'ensemble des livrables (schémas logique et physique, plan d'adressage, configurations sauvegardées, captures, documentation technique) est centralisé dans Nextcloud dans un dossier intitulé *"Dossier Infra Hepturing"*.

  Lien Nextcloud https://192.168.10.5/ ou https://nextcloud/ connexion avec le compte de session du PC.
  L'ensemble des livrables sont aussi sur une clé USB mise à disposition.

MDP KEEPASS : P@ssw0rd

[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.

ANNEXE VII-1-A : Fiche descriptive de réalisation professionnelle (verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Contexte :

Oasis est une entreprise parisienne créée en 2017, spécialisée dans les voyages sur mesure haut de gamme. Elle ouvre une agence à Marseille pour répondre à la demande croissante dans le sud. Les équipes travaillent via mail, téléphone et un cloud interne, avec des postes Windows standardisés. La croissance de l'entreprise nécessite une modernisation informatique pour centraliser, sécuriser et harmoniser les services.

Jusqu'à présent, les connexions réseau se faisaient uniquement via des postes filaires. Afin d'améliorer la mobilité des collaborateurs et de permettre un accès sécurisé à Internet pour les visiteurs, la direction souhaite la mise en place d'une infrastructure Wi-Fi professionnelle au sein des locaux.

Problématique :

Comment mettre en place une solution Wi-Fi professionnelle garantissant à la fois fiabilité, sécurité et segmentation des flux, afin de répondre aux exigences opérationnelles d'une agence en croissance ?

Étude des solutions / choix de la solution

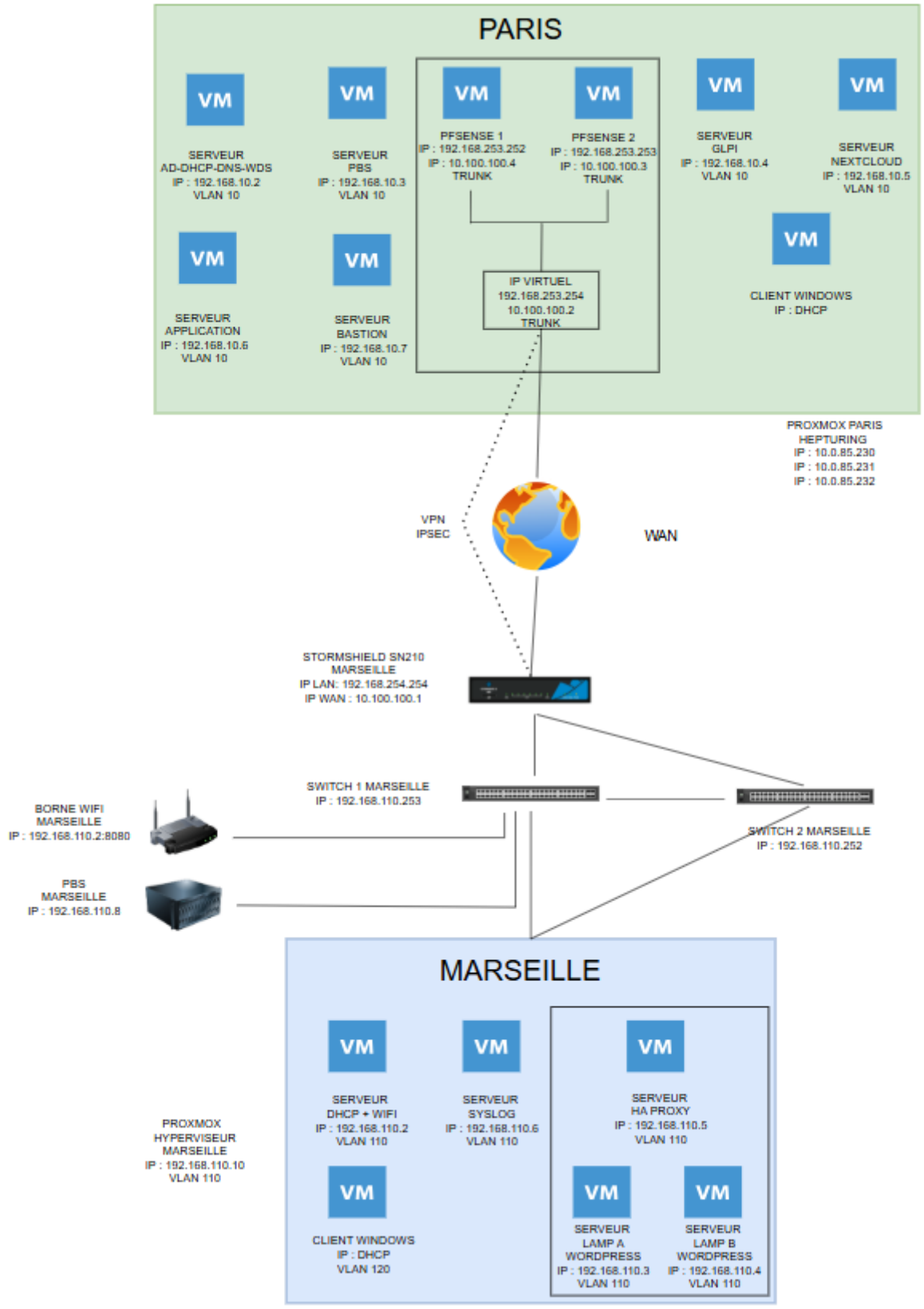
Deux solutions ont été comparées :

- La borne Cisco Catalyst 9105AXI-E offre de meilleures performances mais est plus complexe à administrer.
- La UAP-AC-Lite propose une gestion simple via UniFi Controller, supporte les VLAN et répond largement aux besoins du site.

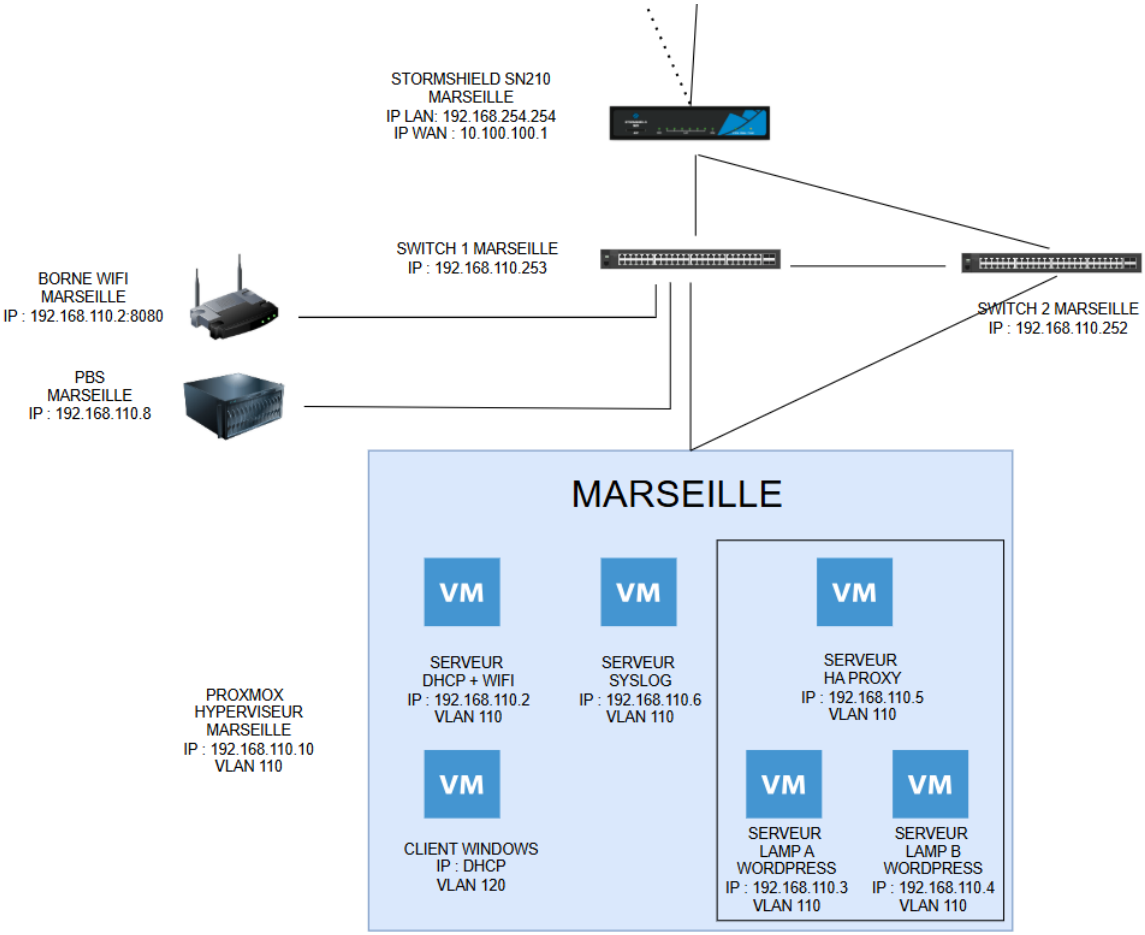
La solution Ubiquiti UAP-AC-Lite a été retenue car elle répond pleinement aux besoins de l'entreprise :

- Gestion centralisée simple via UniFi Controller,
- Prise en charge native des VLAN pour séparer employés et invités,
- Configuration rapide et intuitive,

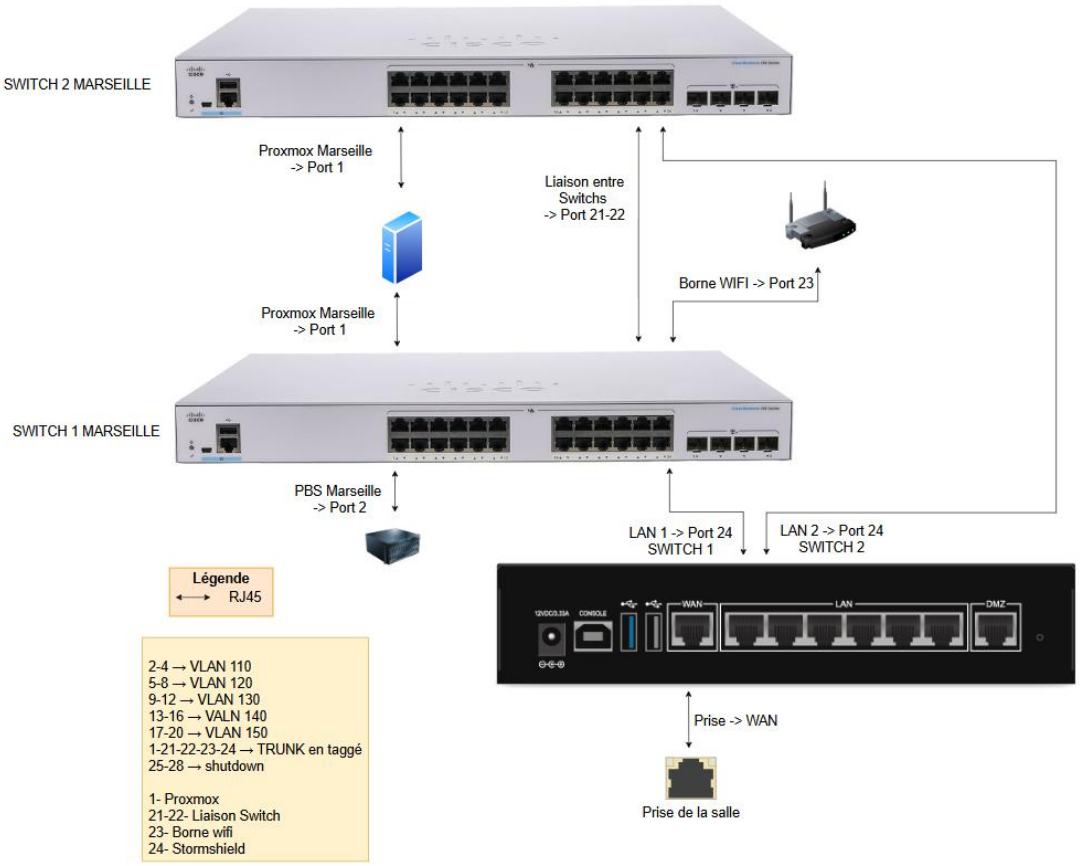
Topologie logique global



Topologie logique wifi



Topologie physique globale



Plan d’adressage

RESEAU	LIEU	VLAN	ROLE	RESEAU	MASQUE	Type d'adressage
LAN	PARIS	10	SERVEUR	192.168.10.1 - 192.168.10.254	255.255.255.0	DHCP
LAN	PARIS	20	POSTE CLIENT	192.168.20.1 - 192.168.20.254	255.255.255.0	DHCP
LAN	PARIS	30	WIFI EMPLOYÉ	192.168.30.1 - 192.168.30.254	255.255.255.0	DHCP
LAN	PARIS	40	WIFI INVITÉ	192.168.40.1 - 192.168.40.254	255.255.255.0	DHCP
LAN	PARIS	50	ADMIN	192.168.50.1 - 192.168.50.254	255.255.255.0	DHCP
LAN	MARSEILLE	110	SERVEUR	192.168.110.1 - 192.168.110.254	255.255.255.0	DHCP
LAN	MARSEILLE	120	POSTE CLIENT	192.168.120.1 - 192.168.120.254	255.255.255.0	DHCP
LAN	MARSEILLE	130	WIFI EMPLOYÉ	192.168.130.1 - 192.168.130.254	255.255.255.0	DHCP
LAN	MARSEILLE	140	WIFI INVITÉ	192.168.140.1 - 192.168.140.254	255.255.255.0	DHCP
LAN	MARSEILLE	150	ADMIN	192.168.150.1 - 192.168.150.254	255.255.255.0	DHCP
WAN	MARSEILLE			10.100.100.1		
WAN	PARIS			10.100.100.2		

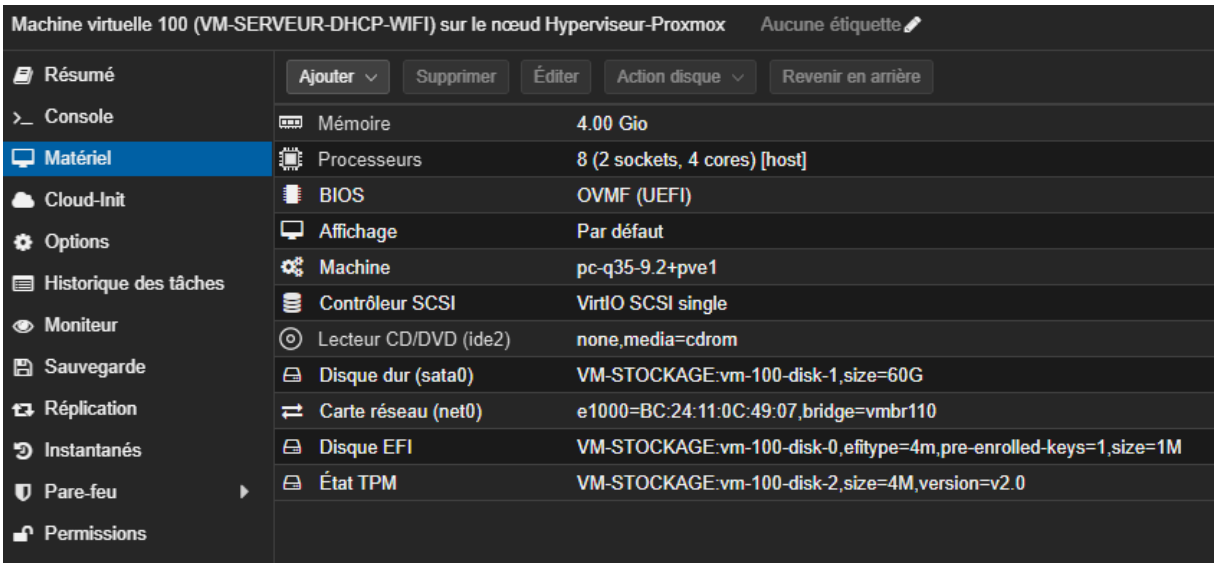
MATERIELS RESEAUX				
Nom de la machine	**IP**	**PORT SWITCH**	**VLAN**	**Notes**
SWITCH-1-Hepturing MARSEILLE	192.168.110.253			SSH: admin
SWITCH-2-Hepturing MARSEILLE	192.168.110.252			SSH: admin
ROUTEUR STORMSHIELD MARSEILLE	10.100.100.1 192.168.254.254	24	TRUNK	
	192.168.110.254	1-4	Vlan 110	
	192.168.120.254	5-8	Vlan 120	
	192.168.130.254	9-12	Vlan 130	
	192.168.140.254	13-16	Vlan 140	
	192.168.150.254	17-20	Vlan 150	
WIFI MARSEILLE	192.168.110.2:8080	23	Vlan 130/140	

PROXMOX MARSEILLE				
				Serveur
Nom de la machine	**Numéro CT/VM**	**Rôle**	**VLAN**	**IP**
PROXMOX MARSEILLE	Proxmox secondaire	Hyperviseur de type 1	110	https://192.168.110.10:8006
VM-AD_REDONDE-DHCP-WIFI	100	RODC + WIFI	110	192.168.110.2
VM-WEB-A	102	SERVEUR WEB A	110	192.168.110.3
VM-WEB-B	103	SERVEUR WEB B	110	192.168.110.4
VM-HAPROXY	104	HA PROXY	110	192.168.110.5
VM-SYSLOG	106	SYSLOG	110	192.168.110.6
				PC Client
VM-Client-Windows	101	PC Client	120	DHCP

Déroulement de la mission en lien avec les compétences

1 -Installation de l'infrastructure de virtualisation

- **Hyperviseur :** Proxmox Virtual Environment 8.4.1
- **Machine :** 100 (VM-SERVEUR-DHCP-WIFI) : Windows Server 2022 Datacenter
- **Ressources allouées :**



Une fois la VM installé j'ai configuré l'IP en 192.168.110.2 afin que la borne Wi-Fi puisse pointer vers le contrôleur sans interruption.

2- Installation du contrôleur Unifi

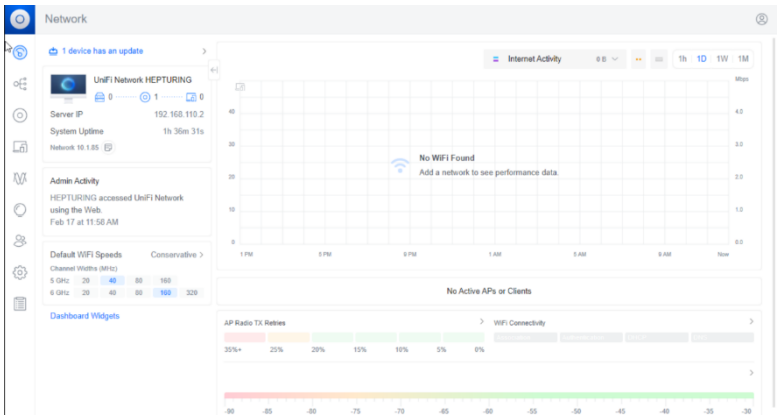
- **Installation de UniFi Controler**

  J'ai installé l'application Unifi Network Application 10.1.85.

J’ai dû installer Microsoft Visual C++ car MongoDB ne démarrait pas afin d’avoir accès à l’interface web.

- **Accès à l’interface web UniFi**

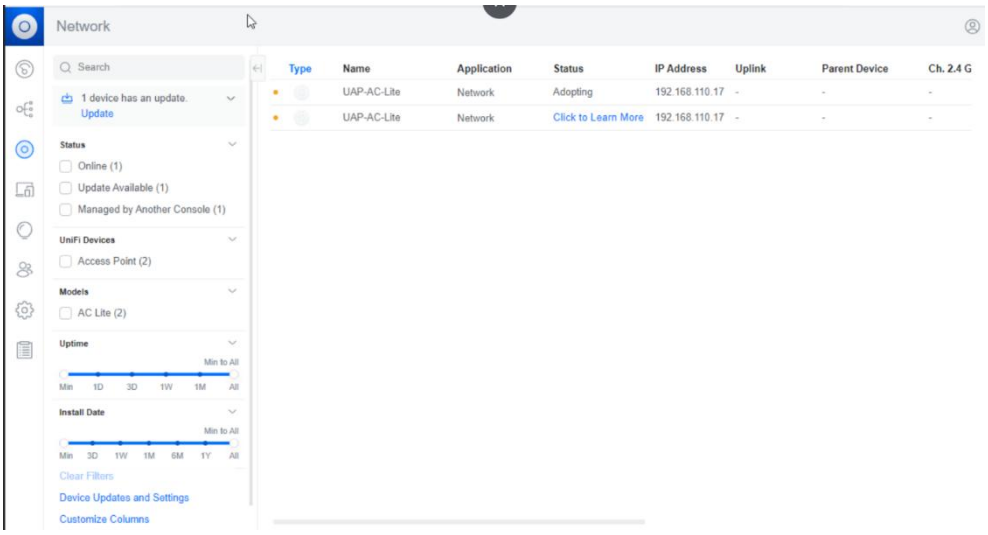
Une fois installé et connecté avec le compte Administrateur, l’accès à l’interface est disponible. On peut aussi se connecter à l’adresse : http://192.168.110.2:8443.



Point important : Si l’interface web UniFi n’est plus accessible, cela signifie que la VM qui héberge le contrôleur est arrêtée. Pour rétablir l’accès, il suffit de relancer la VM ainsi que l’application UniFi Network (version 10.1.85).

3- Adoption de la borne wifi par le contrôleur

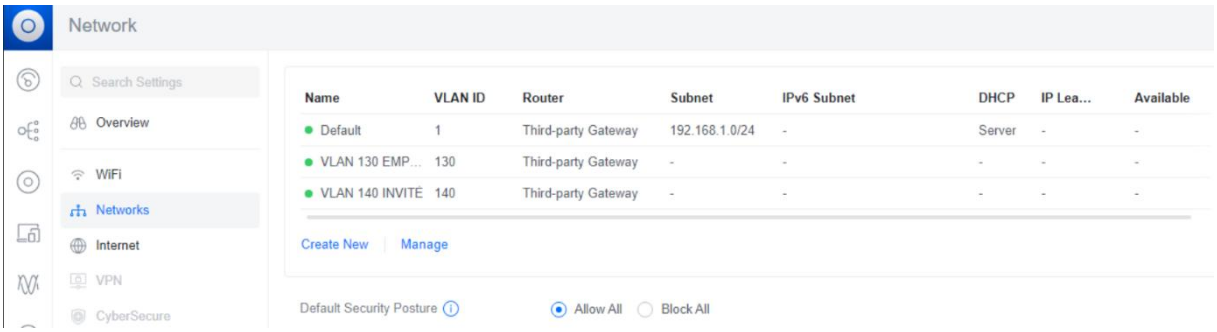
Pour permettre d'ajouter la borne à l'interface Management , il faut effectuer l'adoption, c'est-à-dire la borne passe de l'état "Pending Adoption" à "Connected".



4- Création des VLANs

- **Création des VLANs 130 et 140**

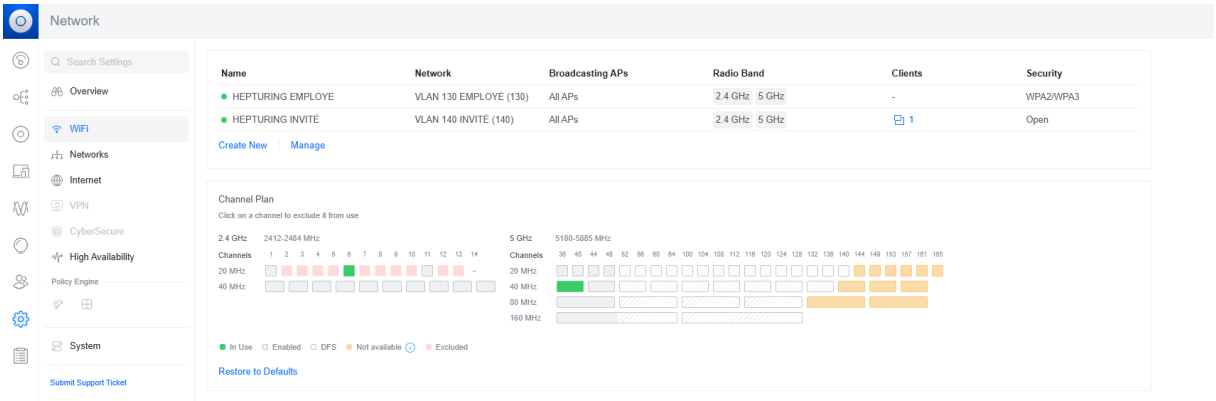
J'ai créé deux VLANs distincts dans l'interface pour la segmentation



5- Configuration des SSID

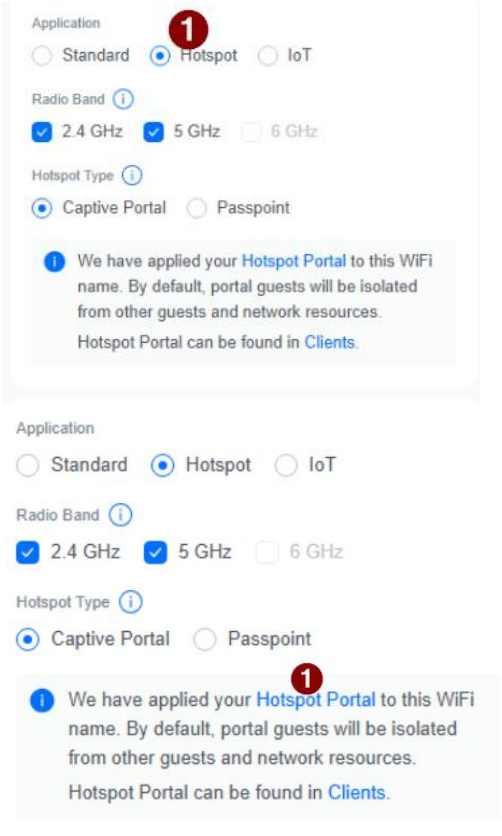
Une fois les VLANS crées, il faut créer les 2 SSID avec leur VLAN associés.

- **EMPLOYÉ**
  - SSID destiné exclusivement au personnel de l'entreprise.
  - Associé au VLAN 130, permettant l'accès aux ressources internes (serveurs, imprimantes, applications métiers).
  - Paramètre des différentes options à cocher :
    - Diffusé en 2,4 GHz et 5 GHz pour assurer une bonne couverture et permettre la connexion d'appareils anciens comme récents.
    - Sécurisé en WPA2/WPA3, assurant compatibilité et haut niveau de protection.
    - PMF en mode Optional, pour renforcer la sécurité tout en évitant les problèmes avec les appareils anciens.
    - Band Steering, BSS Transition et Auto DTIM activés pour optimiser la répartition des clients et améliorer la stabilité du réseau.
- **INVITÉ**
  - SSID destiné aux visiteurs de l'entreprise.
  - Associé au VLAN 140, assurant une isolation complète du réseau interne.
  - Ajout des mêmes paramètres que le SSID Employé sauf :
    - Sécurisé en WPA2/WPA3, où j'ai indiqué ouvert
  - Paramètre supplémentaire :
    - Client Device Isolation activée, empêchant les invités de communiquer entre eux et limitant les risques d'attaque latérale.



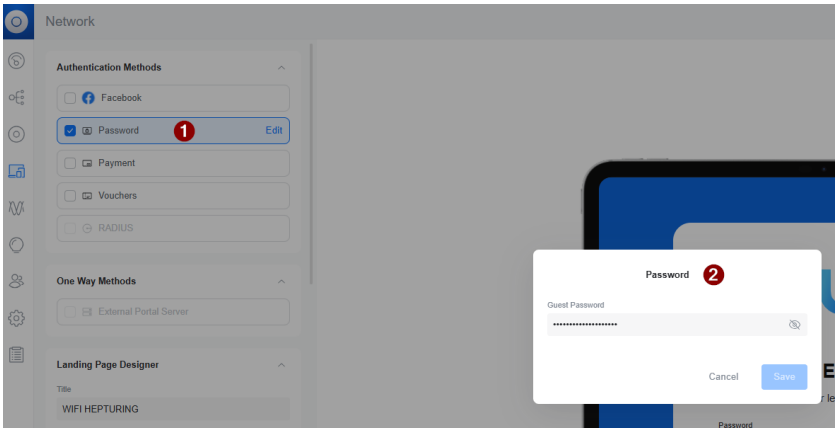
6- Configuration du Portail captif

J'ai mis en place le portail captif qui permet de contrôler l'accès des visiteurs. Il redirige automatiquement les utilisateurs du VLAN 140 vers une page d'authentification avant d'autoriser l'accès à Internet. Cette mesure renforce la sécurité et empêche tout accès non autorisé au réseau interne.

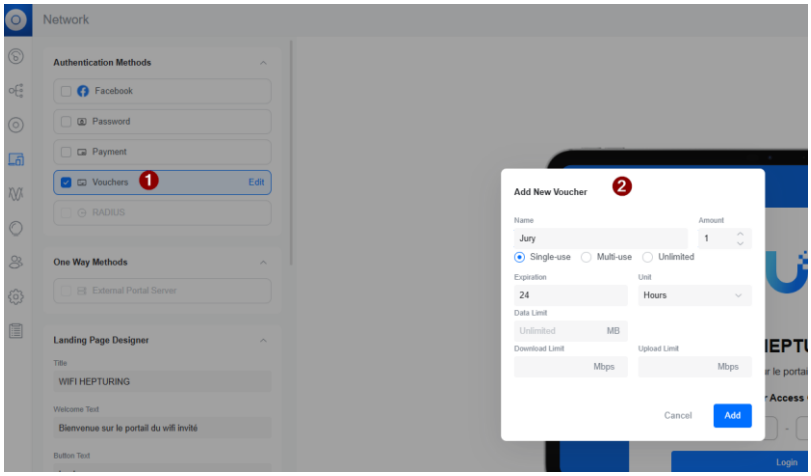


J'ai deux solutions d'Authentification que je peux choisir :

- « Password », ce mode consiste à avoir le seul même mot de passe pour tous les invités. Chaque utilisateur saisit le même code pour accéder au réseau Wi-Fi.



- « Vouchers », ce mode permet de générer un code unique par invité. Chaque voucher peut avoir une durée limitée, un nombre d'utilisations défini, et une expiration automatique.



7- Configuration réseau

- **Switch**

  interface GigabitEthernet1/0/23

  description WIFI

  switchport trunk allowed vlan 110,130,140

  switchport trunk native vlan 110

  switchport mode trunk

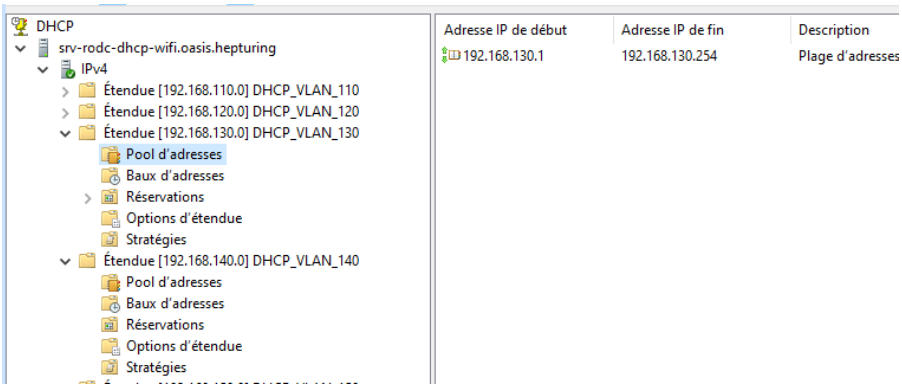
Le VLAN 110 est utilisé comme VLAN natif pour la gestion des équipements réseau (contrôleur, borne, switches). Il permet d'assurer une communication stable entre les équipements d'infrastructure.

L'Interface est en mode TRUNK afin de permettre le transport des VLANs vers la borne Wi-Fi.

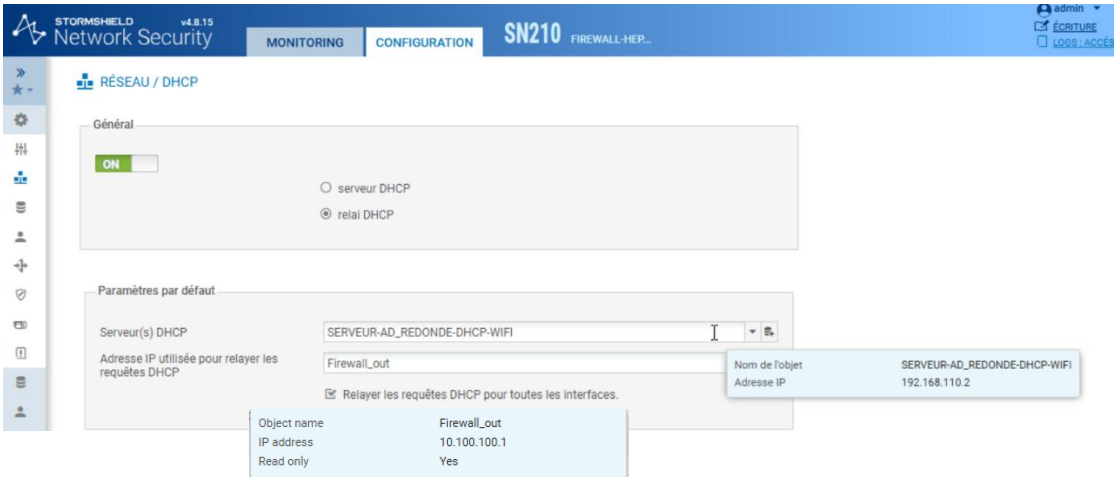
- **DHCP**

Le serveur DHCP est centralisé sur le site de Marseille. Pour permettre aux clients Wi-Fi de Marseille d'obtenir une adresse IP dans leur VLAN respectif (130 ou 140), j'ai configuré :

- **Pools DHCP dans le serveur DHCP de Marseille**



- **Relais DHCP activé sur Stormshield Marseille afin de recevoir les adresses du serveur DHCP**



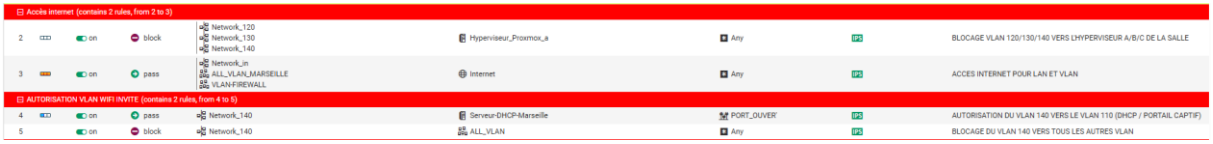
Le relais DHCP transmet les requêtes DHCP des VLAN 130 et 140 vers le serveur DHCP distant, ce qui permet aux clients Wi-Fi d'obtenir automatiquement une adresse IP correspondant à leur réseau.

- **Firewall (Stormshield SN210)**

Pour garantir la sécurité du réseau interne, j'ai mis en place des règles de filtrage sur le Stormshield :

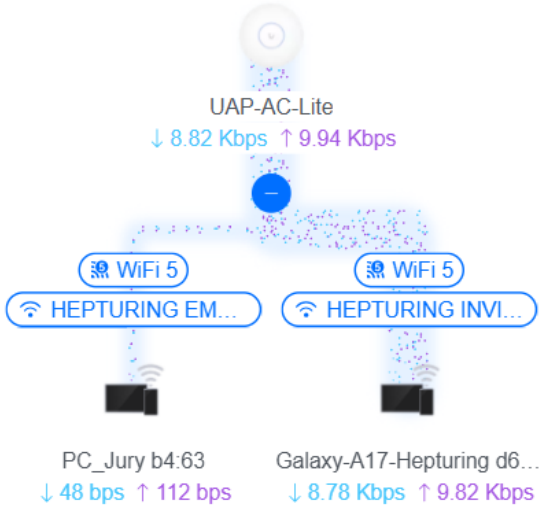
- Le VLAN 140 (invités) est autorisé uniquement vers Internet
- Accès interdit vers les services internes : SMB, RDP, DNS interne, serveurs métiers
- Isolation inter-VLAN : aucun trafic entre VLAN 130 et VLAN 140
- Client Isolation activée sur le SSID invité pour empêcher les visiteurs de communiquer entre eux

Ces règles assurent une séparation totale entre le réseau interne et le réseau invité.



Test

- Test de connexion simultanée



- Test de séparation réseau (exemple : Ping d'un poste connecté au Wifi invité vers l'IP du contrôleur :192.168.110.2)

```
Carte réseau sans fil Wi-Fi :

   Suffixe DNS propre à la connexion. . . : oasis.hepturing
   Adresse IPv6 de liaison locale. . . . .: fe80::3d2f:7610:c6c0:7c3c%5
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.140.6
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.140.254

Carte Ethernet Connexion réseau Bluetooth :

   Statut du média. . . . . . . . . . . . : Média déconnecté
   Suffixe DNS propre à la connexion. . . :

C:\Users\jury01>ping 192.168.110.2

Envoi d'une requête 'Ping'  192.168.110.2 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.110.2:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Conclusion

La mise en place du Wi-Fi professionnel a permis d'améliorer la mobilité interne et d'offrir un accès sécurisé aux visiteurs. La segmentation via VLAN, l'isolation des invités et le portail captif garantissent un niveau de sécurité. La solution Ubiquiti répond pleinement aux besoins de l'agence et reste évolutive pour les futurs déploiements.