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 : 1**
Nom, prénom : SEVESTRE Diwen	**N° candidat : 2302802375**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 29 / 04 / 2026

Organisation support de la réalisation professionnelle
Plateforme pédagogique – Environnement multisites (Paris / Marseille) virtualité sur ProxmoxVE (DSLNetworks)

Intitulé de la réalisation professionnelle
Mise en place d'une infrastructure Wi-Fi centralisée (UniFi Network)

Période de réalisation : 2024 – 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 : L'infrastructure de test comprenait un serveur physique d'hébergement sous Proxmox VE, une licence Windows Server 2022 Standard, une borne Wi-Fi Ubiquiti UniFi UAP-AC-Lite, un switch manageable (liaison Trunk) et un pare-feu FortiGate 50E. L'accès au contrôleur devait être possible via une interface Web centralisée.

Les résultats attendus : L'objectif était de déployer une solution Wi-Fi professionnelle permettant :

- La gestion centralisée des points d'accès via un serveur de contrôle virtualisé.
- La segmentation stricte des flux par VLAN (VLAN 13 pour les employés, VLAN 20 pour les invités).
- La sécurisation des accès via un portail captif et l'activation de l'isolation des clients (Client Isolation) pour le réseau visiteur.
- Une administration accessible à distance pour garantir le maintien en condition opérationnelle

[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 matérielles :**
  - Bornes Wi-Fi Ubiquiti UniFi UAP-AC-Lite.
  - Switch manageable (interconnexion et gestion des VLANs).
  - Pare-feu FortiGate 50E (passerelle et filtrage).
  - Serveur physique d'hébergement (Proxmox VE).
- **Ressources logicielles :**
  - UniFi Network Server (Logiciel de contrôle centralisé).
  - Système d'exploitation : Windows Server 2022 Standard (VM dédiée).
  - Hyperviseur : Proxmox VE
  - Prérequis : Java Runtime Environment (JRE) et Visual C++ Redistributable.
- **Ressources documentaires et outils :**
  - Console de configuration web UniFi.
  - Documentation technique Ubiquiti (Adoption, SSID, Guest Portal).
  - Schémas d'architecture réseau (Logique et Physique).
  - Plan d'adressage IP et tableau des VLANs (60, 13, 20).

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

- **Accès aux ressources techniques et identifiants :**

  - Un PC de démonstration est mis à disposition, incluant un coffre-fort numérique KeePass local. Ce dernier contient l'ensemble des identifiants sécurisés pour l'administration de la VM Windows Server 2022 et du contrôleur UniFi.
  - L'accès aux équipements d'infrastructure s'effectue via un Bastion sécurisé, point d'entrée unique permettant l'administration centralisée du serveur Proxmox, du switch et du pare-feu FortiGate.

- **Accès à la documentation numérique (Nextcloud) :**

  - Une instance Nextcloud dédiée regroupe l'intégralité de la documentation technique du projet. Le jury y trouvera notamment :
    - Le fichier d'adressage IP complet et le tableau des VLANs (60, 13, 20).
    - Les topologies réseau (physique et logique) détaillant l'interconnexion entre le site de Marseille et le cœur de réseau.
    - Les fichiers de configuration et les rapports de tests.

- **Démonstration en direct :**

  - Possibilité de naviguer dans l'interface de gestion UniFi Network Server (via l'URL https://192.168.1.205:8443) pour présenter la configuration des SSID, du portail captif et des règles d'isolation des clients.

---

[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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

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 explicatif

1. CONTEXTE ET PROBLÉMATIQUE

Contexte : Dans le cadre de l'optimisation de l'infrastructure réseau de l'organisation pédagogique d'Oasis, il est devenu nécessaire de déployer une solution Wi-Fi professionnelle. Jusqu'alors, l'accès au réseau se faisait exclusivement en filaire, ce qui limitait la mobilité des collaborateurs et l'accueil des intervenants.

Problématique : Comment offrir un accès sans fil performant, gérable intégralement à distance via une console centralisée, tout en garantissant une sécurité stricte du Système d'Information ? L'enjeu majeur est de permettre une séparation hermétique des flux (Isolation Inter-VLAN) afin que les utilisateurs invités ne puissent en aucun cas atteindre les ressources critiques du réseau interne.

2. ETUDE DES CHOIX DE LA SOLUTION

Le choix s'est porté sur l'écosystème Ubiquiti UniFi en remplacement de l'ancienne infrastructure basée sur des bornes TP-Link. Ce changement s'est avéré indispensable pour les raisons suivantes :

- **Limitation technique de l'existant** : Les bornes TP-Link précédemment en place ne permettaient pas une segmentation avancée. Elles ne pouvaient gérer qu'un seul réseau (VLAN) par borne, rendant impossible l'isolation stricte des flux entre les collaborateurs et les invités.
- **Gestion native des VLANs (Multi-SSID)** : Contrairement à l'ancienne solution, la technologie UniFi permet de diffuser plusieurs réseaux Wi-Fi (SSID) sur une seule borne, en associant chaque réseau à un VLAN différent. Cela garantit une isolation hermétique des flux dès le point d'accès.
- **Administration centralisée** : Le déploiement du UniFi Network Server sur notre infrastructure Windows Server 2022 permet de piloter l'ensemble du parc via une interface unique, là où les anciennes bornes nécessitaient des configurations individuelles.
- **Évolutivité** : Cette architecture facilite l'ajout futur de nouvelles bornes sans reconfiguration lourde, les paramètres de sécurité (VLAN, SSID) étant automatiquement poussés par le contrôleur.

3. RESSOUCES UTILISÉES

- **Matériel** :
  - Bornes UniFi UAP-AC-Lite.
  - Switch manageable (Supportant le mode Trunk).
  - Firewall (Fortigate 50^{E}
  - Serveur physique d'hébergement (Proxmox VE Marseille).
- **Serveur** :
  - Windows Server 2022 Standard (Système d'exploitation de la VM).
- **Logiciel** :
  - UniFi Network Server (v10.1.85).
  - Visual C++ Redistributable (VC_redist.x64)

4. ARCHITECTURE RÉSEAU

4.1. Infrastructure de Virtualisation

Pour garantir la disponibilité du service Wi-Fi et permettre une supervision 24h/24, le contrôleur est hébergé sur une machine virtuelle dédiée :

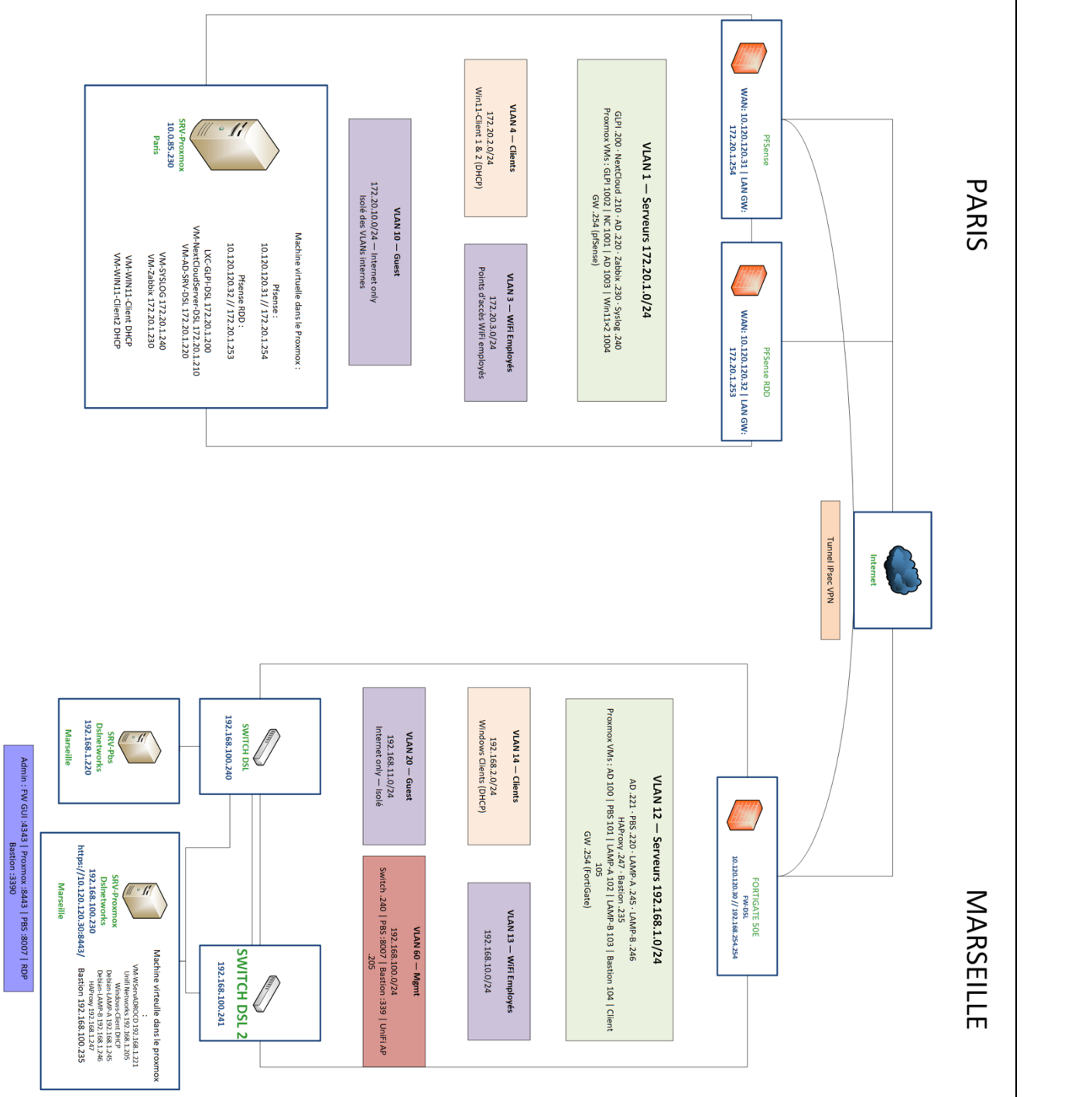
- Hyperviseur : Proxmox VE (Nœud : Proxmox-dslnteworks).
- Machine Virtuelle : VM 106 (VM-SRV-Unifi).
- Ressources allouées : 4 vCPU / 6 Go de mémoire RAM.
- Réseau : L'interface virtuelle de la VM est configurée sur le pont vmbr0 avec un VLAN tag 12 pour isoler les flux de gestion.

4.2. Plan d'adressage et VLANs

Sous Réseaux	Mask	Gateway	Vlan	Site	Description
172.20.1.0	255.255.255.0	172.20.1.254	1	Paris	Serveurs
172.20.2.0	255.255.255.0	172.20.2.254	4	Paris	Poste Clients
192.168.1.0	255.255.255.0	192.168.1.254	12	Marseille	Serveurs
192.168.2.0	255.255.255.0	192.168.2.254	14	Marseille	Poste Clients
192.168.10.0	255.255.255.0	192.168.10.254	13	Marseille	Wifi Employées
192.168.11.0	255.255.255.0	192.168.11.254	20	Marseille	Wifi Invité
192.168.100.0	255.255.255.0	192.168.100.254	60	Marseille	Management

10.120.120.30	255.255.255.0	10.120.120.254		Marseille	Fortigate
10.120.120.31	255.255.255.0	10.120.120.254		Paris	Pfsense 1
10.120.120.32	255.255.255.0	10.120.120.254		Paris	Pfsense 2

4.3. Topologie Logique



Légende

- VLAN Serveurs (vert)
- VLAN Clients / WiFi (violet)
- VLAN Guest (orange)
- VLAN Mgmt (rouge)
- Firewall Paris (pfSense)
- Firewall Marseille (FortiGate)
- Switch / Équipement réseau
- Proxmox / Hyperviseur

Plan d'adressage

Paris

VLAN 1 172.20.1.0/24

VLAN 4 172.20.2.0/24

VLAN 3 172.20.3.0/24

VLAN 10 172.20.10.0/24

Marseille

VLAN 12 192.168.1.0/24

VLAN 14 192.168.2.0/24

VLAN 13 192.168.10.0/24

VLAN 20 192.168.11.0/24

VLAN 60 192.168.100.0/24

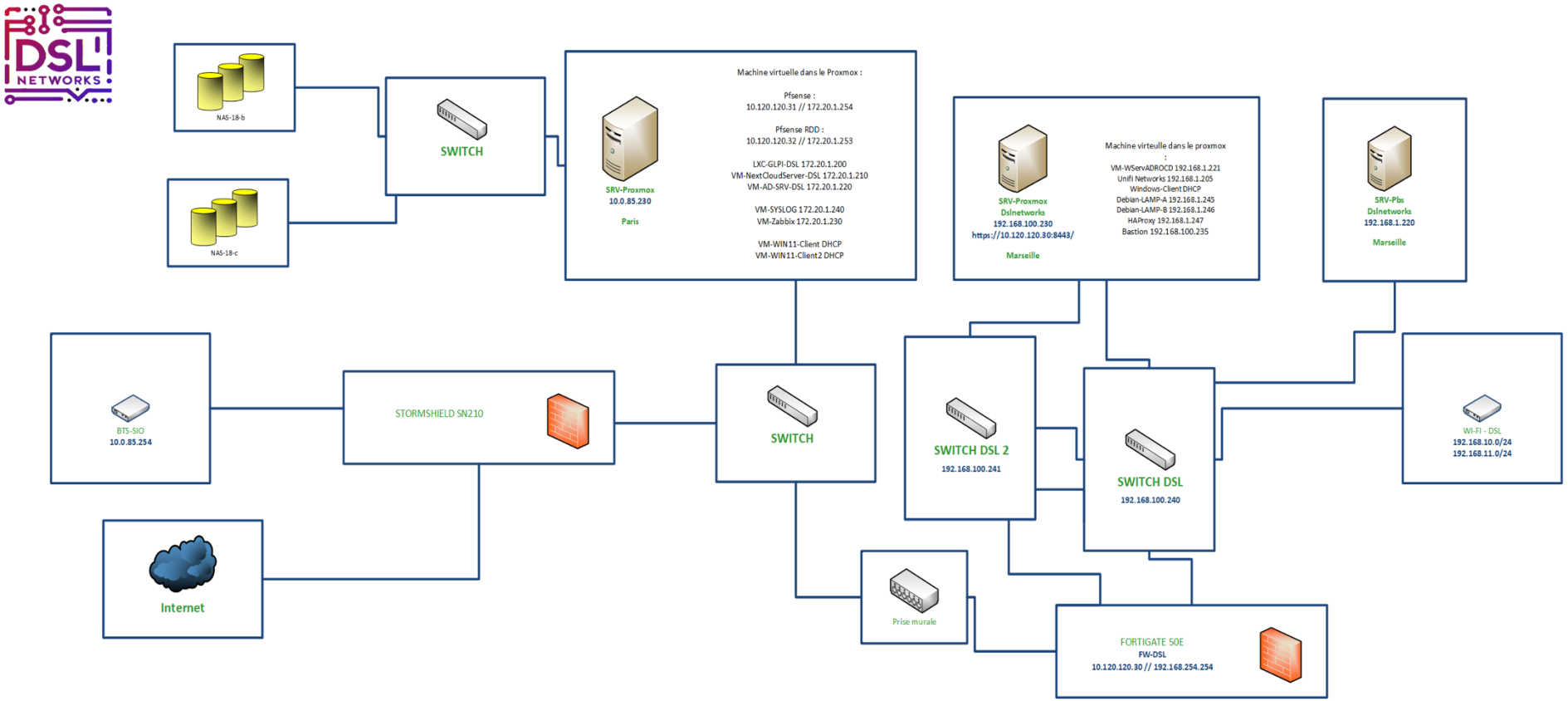
AD : oasis.dslnetworks.local

FW Paris : 10.120.120.31

WAN : 10.120.120.0/24

FW Marseille : 10.120.120.30

4.4. Topologie Physique

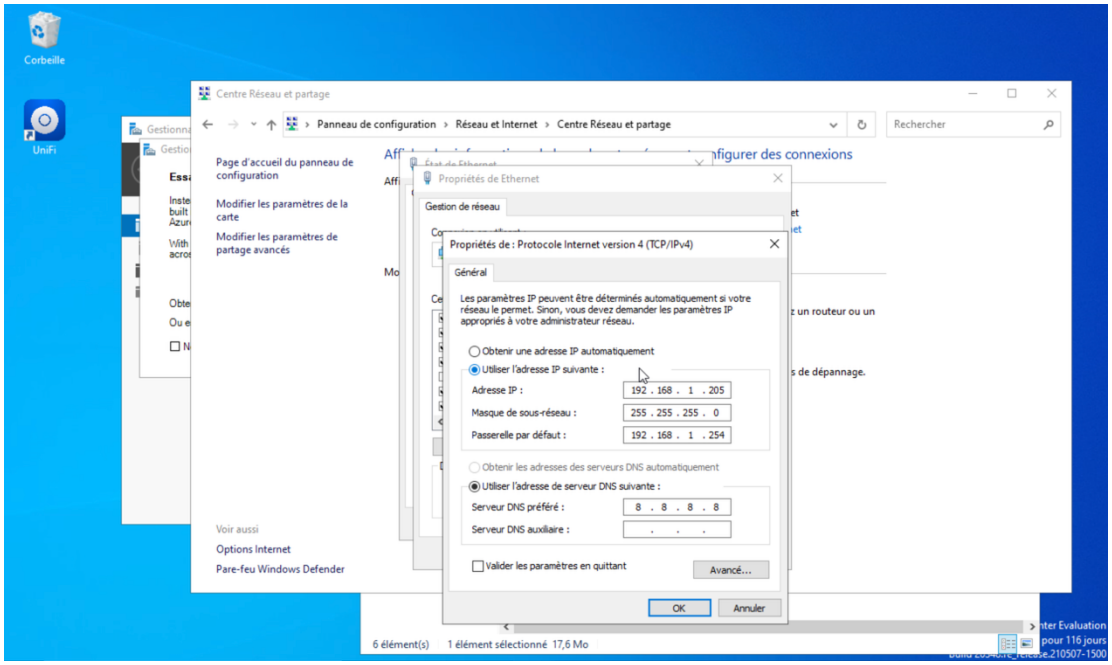


5. RÉALISATION TECHNIQUE

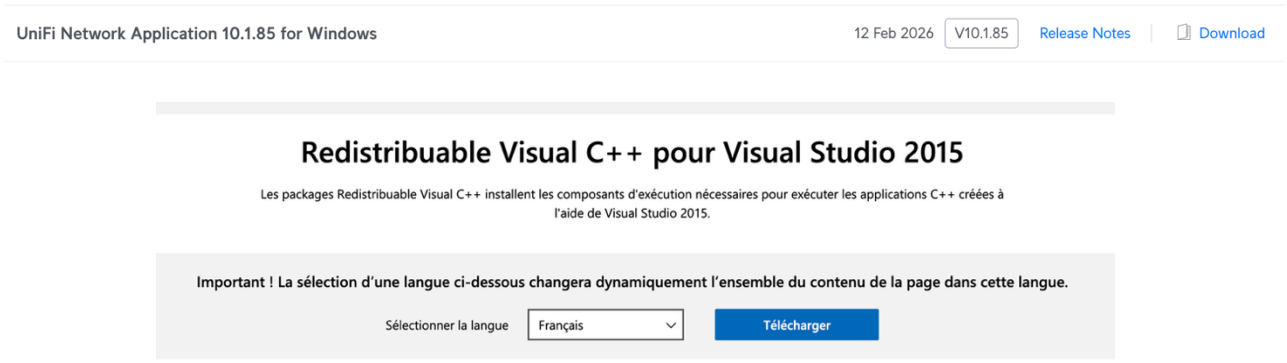
5.1. Préparation du serveur et adressage

Avant l'installation applicative, j'ai configuré la machine virtuelle sous Windows Server 2022 :

- **Adressage Statique** : Fixation de l'IP en 192.168.1.205. Cette IP fixe est indispensable pour que les bornes Wi-Fi puissent pointer vers le contrôleur sans interruption.

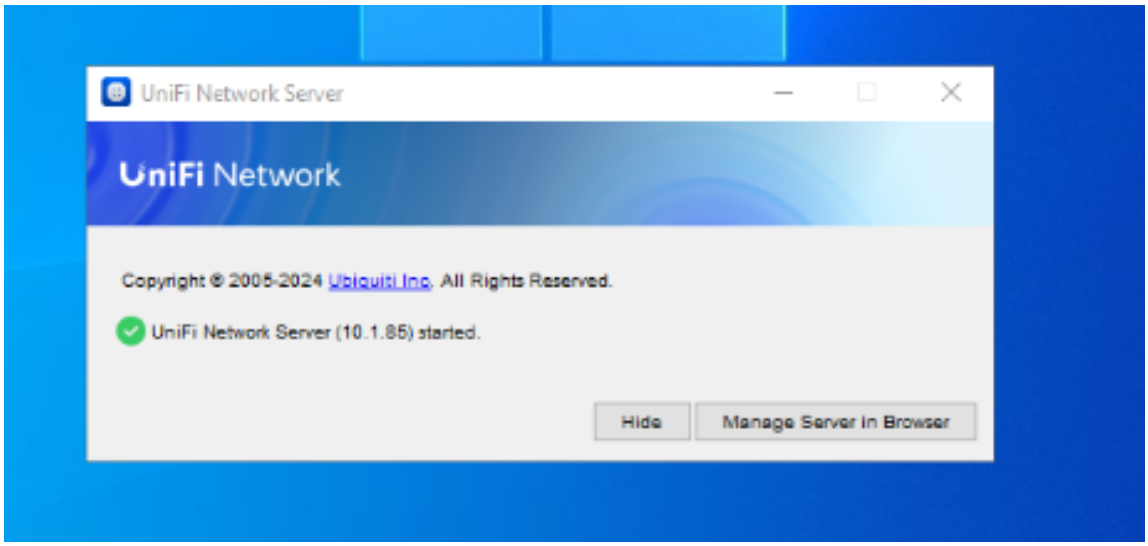


- **Installation des prérequis** : Déploiement du composant Visual C++ Redistributable (requis pour le moteur de base de données MongoDB d'UniFi).

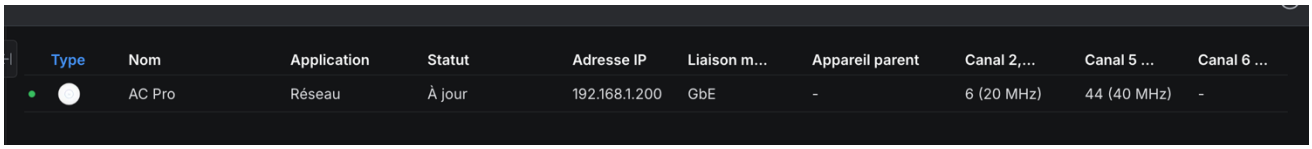


5.1. Installation du Contrôleur UniFi et Connexion à la borne Wifi

Une fois les prérequis validés, j'ai installé l'exécutable « UniFi-installer.exe ». Au premier lancement, le logiciel initialise la base de données et prépare l'interface de gestion web.



Puis sur l'interface Web, j'ajoute la borne wifi a mon Interface Management :

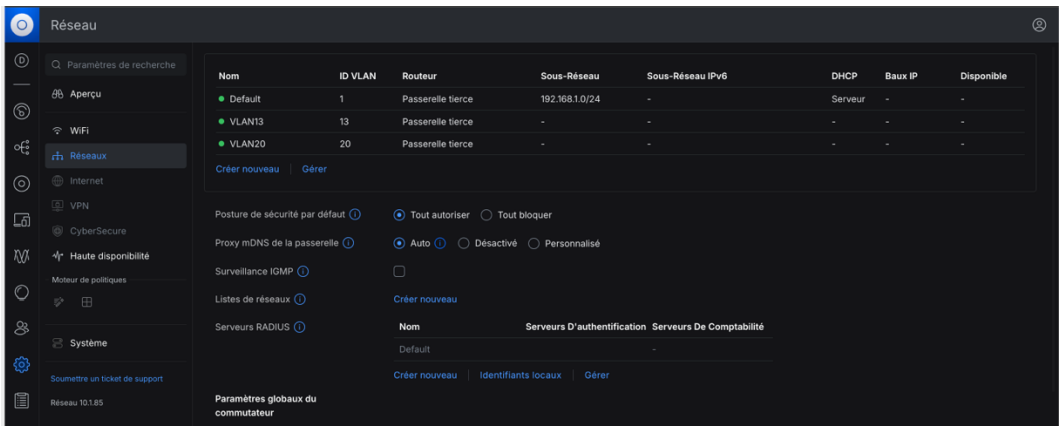


Type	Nom	Application	Statut	Adresse IP	Liaison m...	Appareil parent	Canal 2,...	Canal 5 ...	Canal 6 ...
●	AC Pro	Réseau	À jour	192.168.1.200	GbE	-	6 (20 MHz)	44 (40 MHz)	-

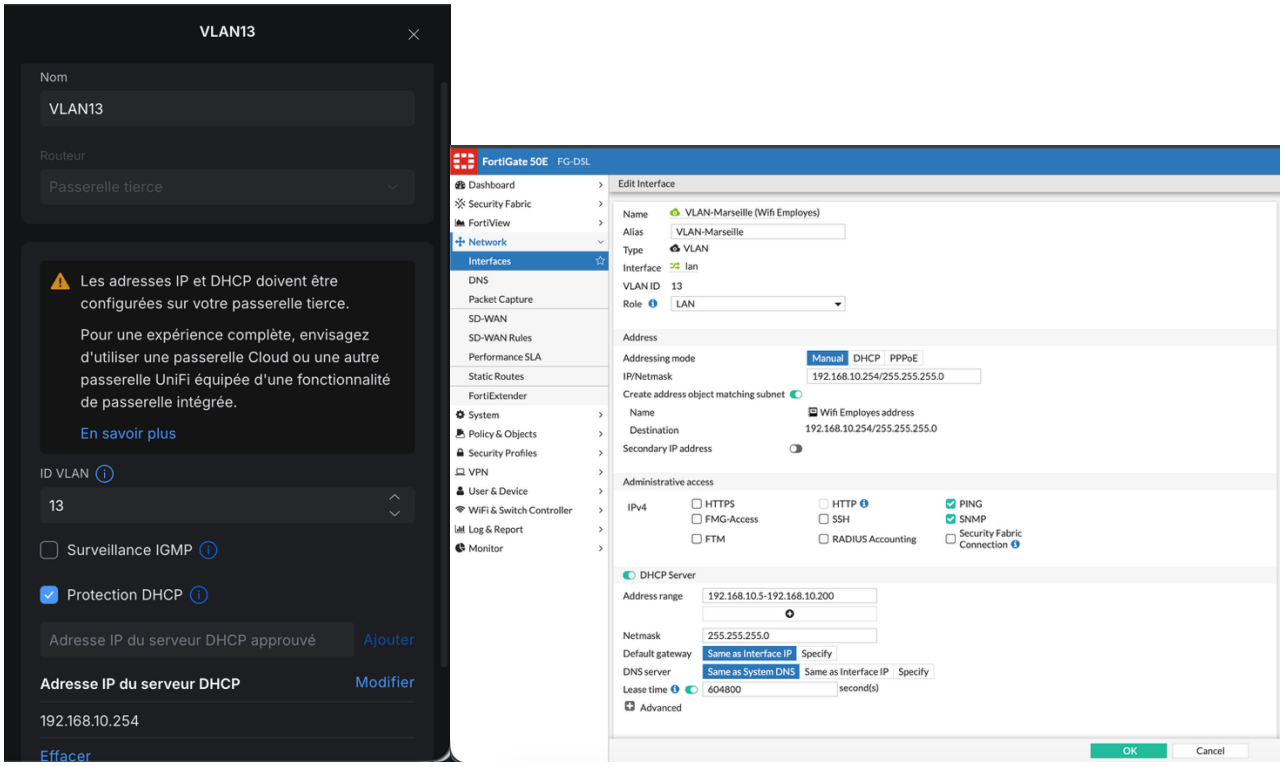
5.2. Configuration des Réseaux (Networks) et VLANs

Pour garantir la sécurité, il ne faut pas que les invités puissent accéder aux serveurs de l'entreprise. J'ai donc créé deux réseaux virtuels (VLANs) distincts dans l'interface UniFi.

- **VLAN 13 (Employés)** : Réseau sécurisé avec accès aux ressources internes.
- **VLAN 20 (Invités)** : Réseau isolé avec accès limité à Internet.



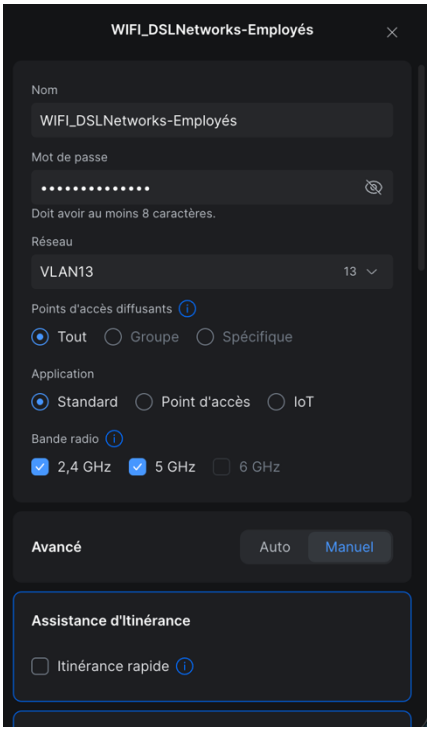
Avec un DHCP automatique depuis notre Fortigate :



5.3. Configuration des SSID (Wireless Networks)

Une fois les réseaux créés, j'ai configuré la borne pour qu'elle diffuse deux noms de réseau Wi-Fi (SSID) différents. Chaque SSID est "étiqueté" (taggué) avec son VLAN correspondant.

1. **SSID "WIFI_DSLNetworks-Employes"** : lié au VLAN 13.
2. **SSID "WIFI_DSLNetworks-Invité"** : lié au VLAN 20.



5.4. Configuration du Switch (Liaison Trunk)

Pour que la borne puisse diffuser ces deux réseaux, le port du switch sur lequel elle est branchée doit être configuré de manière spécifique. Il doit laisser passer le flux de gestion (VLAN 60) et les flux taggués (VLAN 13 et 20).

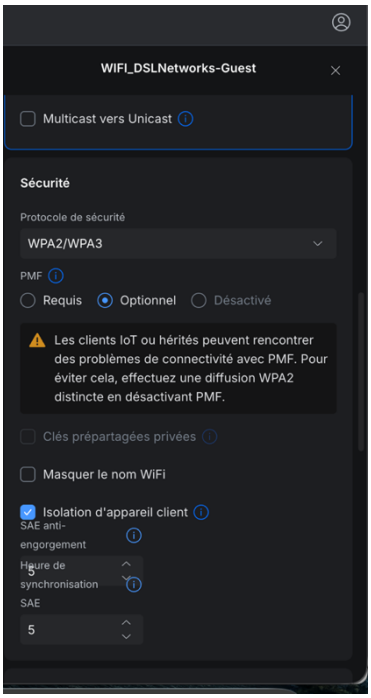
- **Mode du port** : Trunk.
- **VLANs autorisés :** 12,13,20, 60.

```
!
interface GigabitEthernet1/0/23
 description AP_DSLNetworks
 switchport trunk allowed vlan 12,13,20,60
 switchport trunk native vlan 12
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 spanning-tree portfast edge trunk
 ip dhcp snooping trust
!
```

5.5. Sécurisation : Isolation et Filtrage Inter-VLAN

La sécurité du réseau invité repose sur une double protection (Wi-Fi et Pare-feu) pour garantir qu'aucun flux malveillant ne puisse atteindre le cœur du réseau :

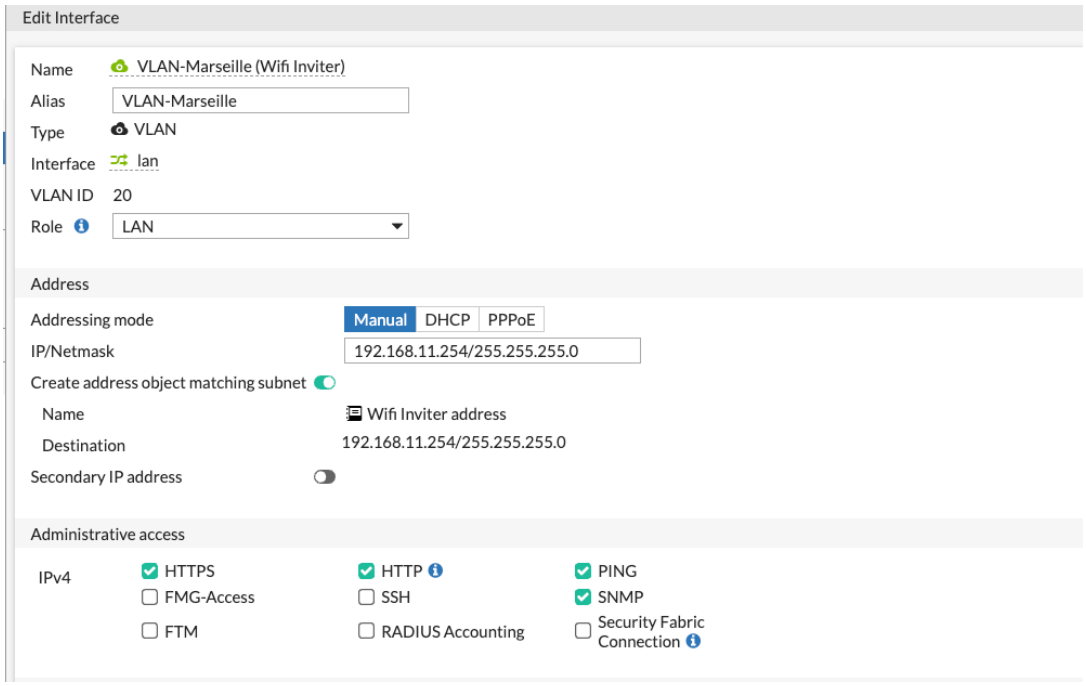
- **Isolation des clients :** Directement sur le contrôleur UniFi, j'ai activé l'option Client Isolation sur le SSID "Guest". Cette fonctionnalité empêche deux appareils connectés au Wi-Fi "Invité" de communiquer entre eux, limitant ainsi les risques de propagation de malwares ou d'attaques latérales entre visiteurs.



- **Filtrage sur le Pare-feu Fortigate :** Pour renforcer cette isolation, j'ai configuré des règles de filtrage strictes sur le Fortigate de l'organisation :
    - **Règle de sortie :** Autorisation du trafic provenant du VLAN 20 uniquement vers l'interface WAN (Internet).

    - **Règle d'interdiction :** Blocage explicite de tout flux provenant du VLAN 20 vers les autres segments du réseau (VLAN 13 Employés, VLAN 60 Management).

    - **Services restreints :** Seuls les services de base (DNS, HTTP, HTTPS) sont autorisés pour assurer la navigation web, tout en interdisant les protocoles sensibles (SMB, RDP, SSH) vers l'extérieur.



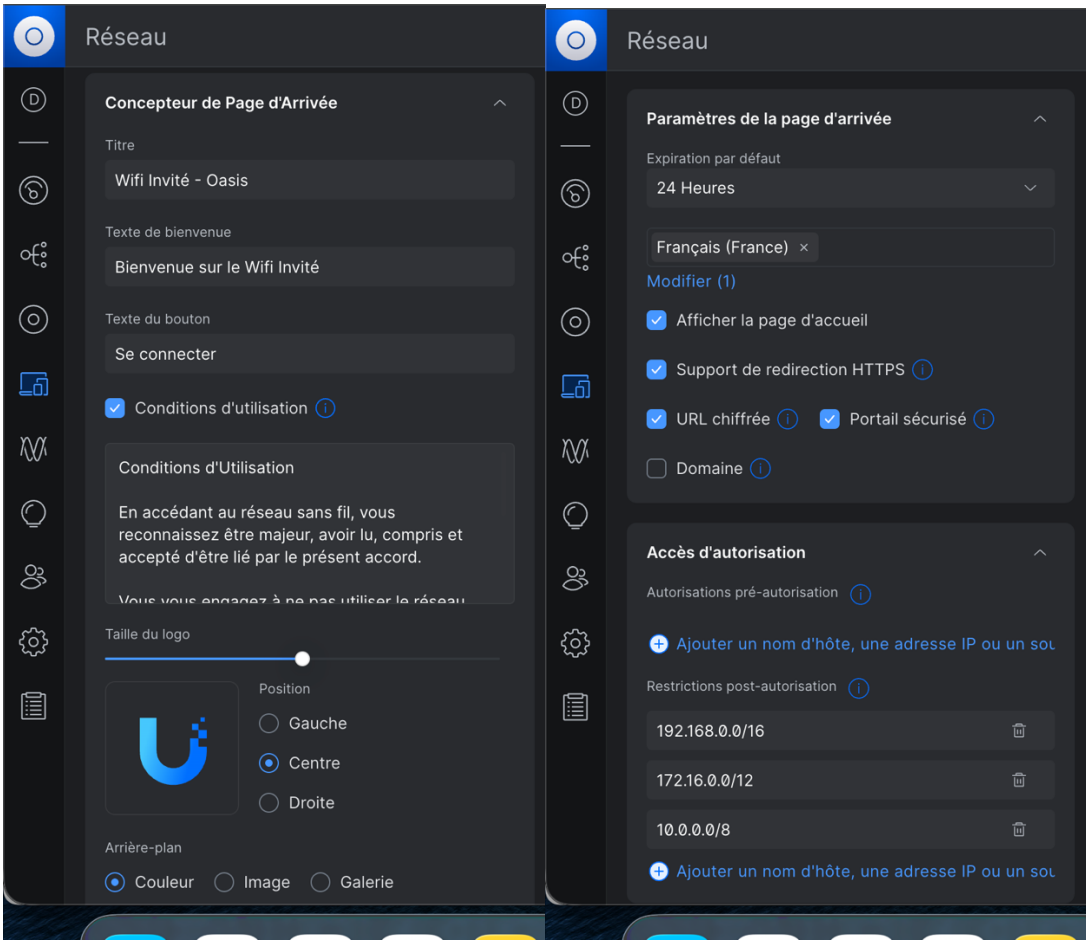
5.6. Mise en place du Portail Captif (Wifi Invité)

Pour le réseau invité, j'ai configuré un portail captif (Hotspot Portal) afin de sécuriser l'accès et de dégager la responsabilité de l'organisation.

- **Personnalisation :** Intégration d'un message de bienvenue et des conditions d'utilisation.
- **Conditions d'utilisation (Terms of Use) :** J'ai configuré l'affichage obligatoire des termes suivants en français :

"En accédant au réseau sans fil, vous reconnaissez être majeur, avoir lu, compris et accepté d'être lié par le présent accord. Vous vous engagez à ne pas utiliser le réseau sans fil à des fins illicites et assumez l'entière responsabilité de vos actes. Le réseau sans fil est fourni « en l'état », sans aucune garantie d'aucune sorte, expresse ou implicite."

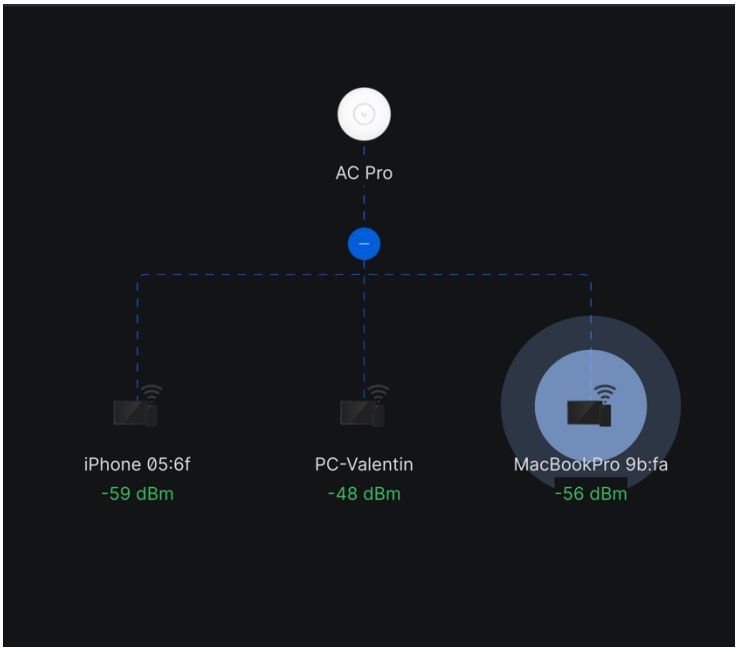
- **Authentification :** L'accès est validé par l'acceptation de ces conditions, permettant ainsi de tracer les connexions si nécessaire.



6. PHASE DE TESTS ET VALIDATION

Afin de valider la conformité de l'installation par rapport aux besoins exprimés, j'ai réalisé une série de tests fonctionnels et de sécurité :

- **Test de connexions simultanées :** Connexion de plusieurs terminaux (PC, smartphone) sur une même borne pour valider la gestion de la charge.



- **Test de séparation réseau (Isolation Inter-VLAN) :** Tentative de "Ping" depuis un appareil connecté au SSID "Guest" vers l'IP du contrôleur (192.168.1.205)

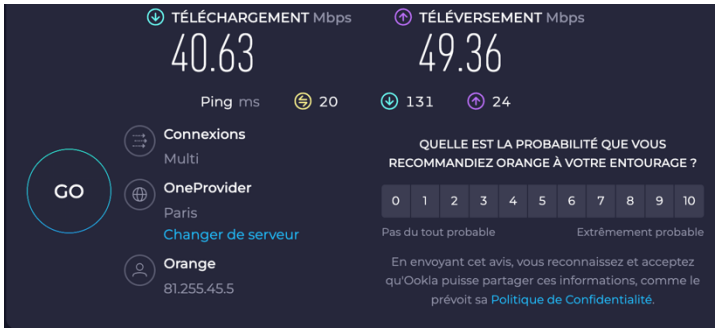
```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6460<TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 06:ca:f9:da:7a:e4
        inet6 fe80::cba:2c90:a3f5:98e9%en0 prefixlen 64 secured scopeid 0xe
        inet 192.168.11.6 netmask 0xffffff00 broadcast 192.168.11.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
diwen@MacBook-Pro-Diwen ~ % ping 192.168.1.205
PING 192.168.1.205 (192.168.1.205): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
Request timeout for icmp_seq 4
Request timeout for icmp_seq 5
Request timeout for icmp_seq 6
Request timeout for icmp_seq 7
^C
--- 192.168.1.205 ping statistics ---
9 packets transmitted, 0 packets received, 100.0% packet loss
```

Ou un poste "Employé" :

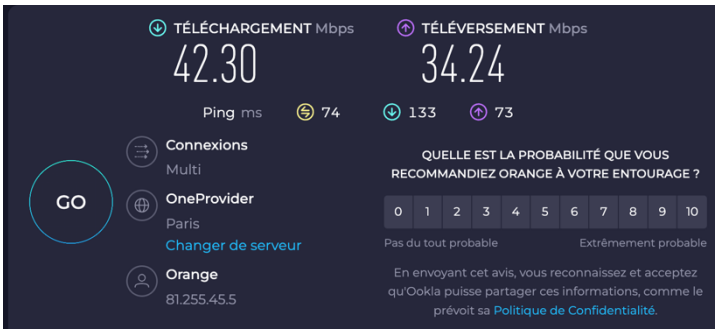
```
diwen@MacBook-Pro-Diwen ~ % ping 192.168.10.6
PING 192.168.10.6 (192.168.10.6): 56 data bytes
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
^C
--- 192.168.10.6 ping statistics ---
5 packets transmitted, 0 packets received, 100.0% packet loss
```

- **Test de débit (Speedtest) :** Mesure de la bande passante sur chaque SSID.

WIFI_DSLNetworks-Employés :



WIFI_DSLNetworks-Invités :



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 : SEVESTRE Diwen	**N° candidat : 2302802375**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date :** 29 / 04 / 2026

Organisation support de la réalisation professionnelle
Plateforme pédagogique – Environnement multisites (Paris / Marseille) virtualité sur ProxmoxVE (DSLNetworks)

Intitulé de la réalisation professionnelle
Mise en place d'un switch

Période de réalisation 2024 – 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[5] (ressources fournies, résultats attendus)

- Les ressources disponibles incluaient un switch manageable Cisco 1000, un firewall Fortigate 50E, un serveur Proxmox, un réseau segmenté en VLANs et un accès administrateur via SSH.
- Les résultats attendus étaient la création d'une architecture réseau segmentée, sécurisée, administrable à distance et disposant d'un mécanisme de redondance.

Description des ressources documentaires, matérielles et logicielles utilisées[6]

- Switch manageable Cisco 1000
- Firewall Fortigate 50E
- Serveur Proxmox
- VLANs 1 à 60
- Console de configuration / SSH
- Documentation Cisco (STP, VLAN, SSH, port-security)
- Schémas logiques et physique

[5] 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.

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

Modalités d'accès aux productions[7] et à leur documentation[8]

- **Accès aux ressources techniques et identifiants :**

  - Un PC de démonstration est mis à disposition lors de l'épreuve. Il contient un coffre-fort numérique KeePass local regroupant tous les identifiants d'administration (Switch, FortiGate, Proxmox).
  - L'administration des équipements (Switch Cisco et Firewall FortiGate) s'effectue via un Bastion sécurisé. Ce point d'entrée unique permet d'établir des liaisons SSH vers la console de configuration du switch et d'accéder à l'interface HTTPS du pare-feu.

- **Accès à la documentation numérique (Nextcloud) :**

  - L'intégralité des livrables est centralisée sur une instance Nextcloud. Le jury pourra y consulter :
    - Les schémas d'architecture (Topologies logique et physique) de l'agence de Marseille.
    - Le tableau d'adressage IP détaillé et la configuration des VLANs (12, 13, 14, 20, 60).
    - Les rapports d'audit et les fichiers de configuration sauvegardés.

- **Démonstration en direct (CLI et Web) :**

  - Présentation de la configuration en ligne de commande (CLI) du switch pour vérifier l'état des ports Trunk, de l'EtherChannel et du Spanning-Tree.
  - Navigation sur l'interface d'administration du FortiGate pour présenter les règles de filtrage inter-VLAN et les politiques de sécurité mises en œuvre pour le site de Marseille.

---

[7] 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.

[8] 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.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

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

1. CONTEXTE ET PROBLÉMATIQUE

Contexte : Dans le cadre de l'ouverture de la nouvelle agence de Marseille, j'ai été chargé de mettre en place l'infrastructure réseau locale. Cette agence doit être autonome tout en restant connectée aux ressources du siège. Le réseau repose sur un switch central administrable qui doit interconnecter un hyperviseur Proxmox (hébergeant le contrôleur Wi-Fi), une borne Wi-Fi UniFi et un pare-feu Fortigate assurant la sortie internet et la sécurité.

Problématique : Comment configurer une infrastructure de commutation robuste capable de segmenter les flux (VLAN), d'assurer la communication entre les serveurs et les bornes, tout en garantissant une sécurité périmétrique via le Fortigate ?

2. ETUDE DES CHOIX DE LA SOLUTION

Le choix s'est porté sur un switch manageable de niveau 2 pour permettre :

- **La segmentation par VLAN :** Indispensable pour isoler le réseau "Employés" du réseau "Invités" et du "Management".
- **Le mode Trunk (802.1Q) :** Nécessaire pour transporter plusieurs réseaux sur un seul câble vers le Fortigate et la borne Wi-Fi.
- **La gestion à distance (SSH) :** Pour administrer l'équipement depuis le siège sans déplacement physique.

3. RESSOUCES UTILISÉES

- **Matériel :** Switch Cisco C1000, Borne UniFi, Pare-feu Fortigate**.**
- **Logiciel :** PuTTY/Terminal (Console série), Navigateur Web (Interface Fortigate/UniFi)

4. ARCHITECTURE RÉSEAU

4.1. Topologie de l’agence de Marseille

Le switch interconnecte les éléments critiques :

1. **Vers le Fortigate :** Liaison Trunk pour le routage Inter-VLAN et la sortie Internet**.**
2. **Vers le Proxmox :** Port d'accès pour le serveur hébergeant le contrôleur**.**
3. **Vers la Borne Wi-Fi :** Liaison Trunk pour diffuser les SSIDs taggués

4.2. Plan d’adressage et VLANs

Voir réalisation numéro 1.

4.3. Topologie Logique et Physique

Voir réalisation numéro 1.

5. RÉALISATION TECHNIQUE

5.1. Initialisation et sécurisation d’accès

La configuration s'effectue via un câble console et le logiciel PuTTY (Baud rate 9600). J'ai configuré le nom d'hôte et sécurisé le mode privilégié avec un mot de passe chiffré

```
Switch-DSLNetworks#show running-config
Building configuration...

Current configuration : 9349 bytes
!
! Last configuration change at 07:58:56 UTC Wed Apr 29 2026 by admin
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname Switch-DSLNetworks
!
boot-start-marker
boot-end-marker
!
!
username admin privilege 15 secret 9 $9$guSDtC5nXT5FZ.$/S4RgCSMeTgRT7Ry7J97KVTEw5LjLso2OmT2Xnk1/Ek
no aaa new-model
switch 1 provision c1000-24t-4g-l
system mtu routing 1500
ip routing
```

5.2. Configuration des VLANs et de l'IP de gestion

J'ai déclaré les VLANs (12, 13, 14, 20, 60) et assigné une adresse statique à l'interface VLAN 60 pour permettre l'administration SSH.

- Interface vlan 60
- ip address 192.168.100.250 255.255.255.0

```
interface Vlan12
 no ip address
!
interface Vlan13
 no ip address
!
interface Vlan14
 no ip address
!
interface Vlan20
 no ip address
!
interface Vlan60
 ip address 192.168.100.240 255.255.255.0
!
interface Vlan120
 no ip address
!
ip default-gateway 192.168.100.254
ip http server
ip http banner
ip http secure-server
ip route 0.0.0.0 0.0.0.0 192.168.100.254
ip ssh time-out 60
ip ssh version 2
!
```

5.3. Configuration des ports TRUNK (Cœur de réseau)

Pour assurer la communication entre le Pare-feu et la Borne Wi-Fi, les ports correspondants sont passés en mode Trunk.

- **Vers FortiGate** : Autorisation de tous les VLANs pour le routage.
- **Vers Borne UniFi** : Mode Trunk avec VLAN 60 en natif pour l'administration de la borne.

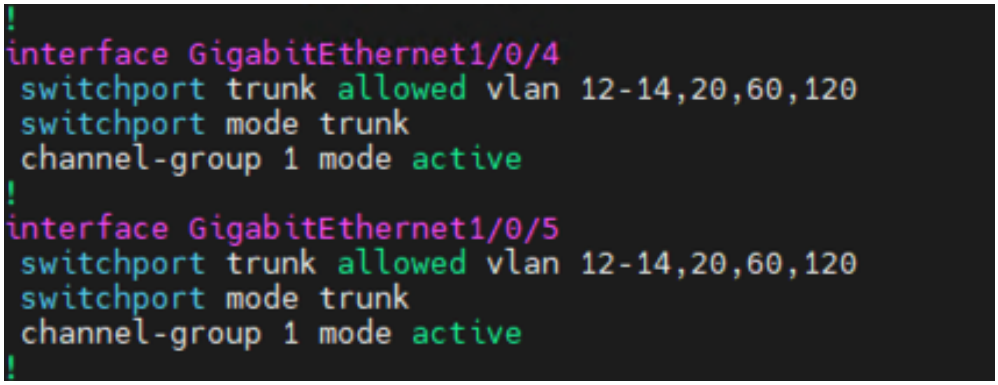
```
!
interface GigabitEthernet1/0/22
 description Vers Proxmox (TRUNK)
 switchport trunk allowed vlan 4,12-14,20,60,120
 switchport trunk native vlan 60
 switchport mode trunk
 spanning-tree portfast edge trunk
 spanning-tree bpduguard enable
!
interface GigabitEthernet1/0/23
 description AP_DSLNetworks
 switchport trunk allowed vlan 12,13,20,60
 switchport trunk native vlan 12
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 spanning-tree portfast edge trunk
 ip dhcp snooping trust
!
interface GigabitEthernet1/0/24
 description Vers Firewall
 switchport access vlan 60
 switchport trunk allowed vlan 2,12-14,20,60,120
 switchport mode trunk
 spanning-tree portfast edge
!
```

5.4. Configuration des ports pour la redondance (EtherChannel)

Afin de garantir une haute disponibilité et d'augmenter la bande passante entre le switch et le reste de l'infrastructure (vers un second switch ou le serveur Proxmox), j'ai mis en place une agrégation de liens logiques via le protocole LACP (Link Aggregation Control Protocol).

- **Objectif :** Fusionner deux liens physiques en une seule interface logique appelée Port-Channel. Cela permet de doubler le débit théorique et d'assurer une continuité de service : si l'un des deux câbles est déconnecté, le trafic bascule instantanément sur le second sans coupure réseau.

- **Configuration réalisée :** * Sélection des interfaces physiques concernées (ex: GigabitEthernet 1/0/4 et 1/0/5).
    - Assignation au groupe de canal avec le mode active pour forcer la négociation LACP.
    - Configuration de l'interface interface port-channel 1 en mode **Trunk** pour laisser passer tous les VLANs de l'agence (12, 13, 14, 20, 60, 120).



6. PHASE DE TESTS ET VALIDATION

- **Vérification de la segmentation :** Commande show vlan brief pour confirmer que chaque port est dans le bon VLAN.

```
Switch-DSLNetworks#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/25, Gi1/0/26, Gi1/0/27, Gi1/0/28
2    VLAN0002                         active
10   WIFI_EMPLOYES                    active
11   WIFI_INVITES                     active
12   VLAN0012                         active    Gi1/0/19
13   VLAN0013                         active
14   VLAN0014                         active
20   VLAN0020                         active
60   VLAN0060                         active    Gi1/0/13, Gi1/0/21
100  VLAN0100                         active
120  VLAN0120                         active    Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/6, Gi1/0/7, Gi1/0/8, Gi1/0/9, Gi1/0/10, Gi1/0/11, Gi1/0/12, Gi1/0/14, Gi1/0/15, Gi1/0/16, Gi1/0/17, Gi1/0/18, Gi1/0/20
```

Show etherchannel summary :

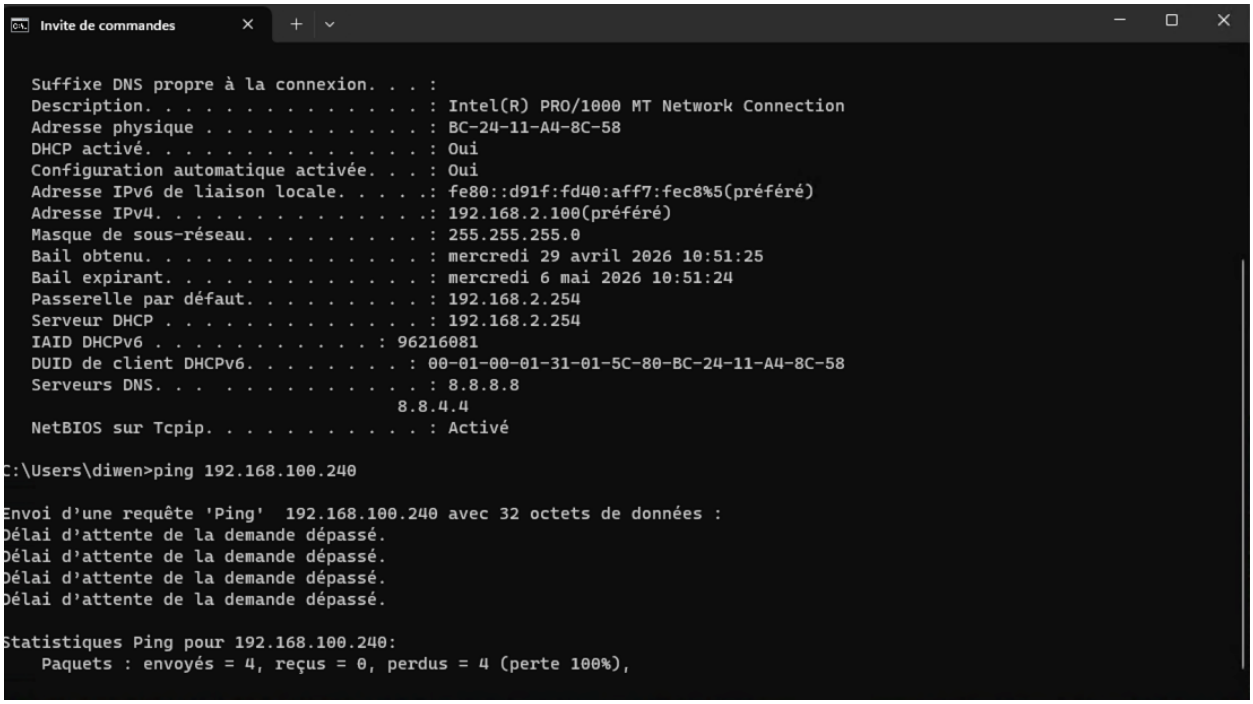
```
Switch-DSLNetworks#show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator

        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Gi1/0/4(P)  Gi1/0/5(P)
```

- **Test de routage :** Ping depuis le switch vers l'interface LAN du FortiGate (192.168.100.254).

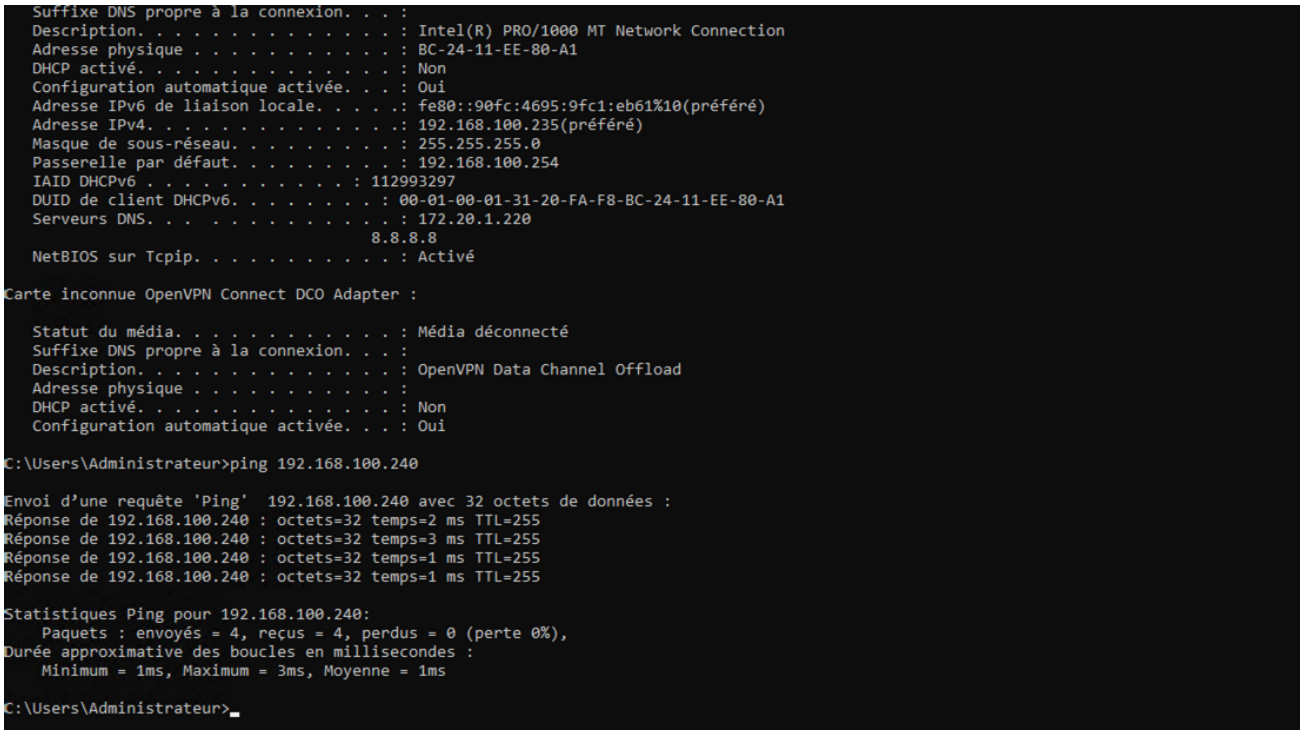
```
Switch-DSLNetworks#ping 192.168.100.254
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.100.254, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 2/3/6 ms
```

- **Test Wi-Fi :** Vérification qu'un client (Employés) reçoit bien une IP via le DHCP du Forti-Gate dans le VLAN 14 + ping vers Switch :

  Ping : NOK



Ping du Bastion au Switch : OK



7. CONCLUSION

La réalisation de cette mission a permis de déployer une infrastructure réseau robuste et cohérente pour la nouvelle agence de Marseille. Ce projet m'a donné l'opportunité de mettre en pratique des concepts clés de l'administration réseau :

- **La segmentation de niveau 2 :** Garantissant l'étanchéité des flux via une gestion rigoureuse des VLANs.
- **La haute disponibilité :** Grâce à la mise en œuvre de l'EtherChannel et du protocole Spanning-Tree, assurant une redondance matérielle et une optimisation de la bande passante entre le cœur de réseau et les accès.
- **La sécurisation périmétrique :** Par l'interconnexion avec le pare-feu Fortigate, permettant un filtrage granulaire des accès internet et inter-VLAN.

Ce déploiement répond non seulement aux besoins immédiats de mobilité et de connectivité de l'agence, mais offre également une architecture évolutive, capable de supporter l'ajout futur de nouveaux services virtualisés sur Proxmox sans compromettre la sécurité globale du Système d'Information.

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2026**

ANNEXE VII-7 : Modèle d'attestation de respect de l'annexe II.E – Environnement technologique pour la certification du référentiel

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

CONTRÔLE DE L'ENVIRONNEMENT TECHNOLOGIQUE

En référence à l'annexe II.E « Environnement technologique pour la certification » du référentiel du BTS SIO

Identification[1]	**Diwen Sevestre** **Valentin Amelie**	**SISR**

1. Environnement commun aux deux options

1.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un service d'authentification	Active Directory	
Un SGBD	MariaDB qui gère la BDD de GLPI	
Un accès sécurisé à internet	Fortigate et PFSense	
Un environnement de travail collaboratif	Partage de fichiers via NextCould	
Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	Windows Server et Debian	

[1] Nom et adresse du centre d'examen ou identification de la personne candidate individuelle (numéro, nom, prénom)

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution de sauvegarde	Proxmox Backup Server (PBS)	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Partage de fichiers par rapport au Groupe associé a l'utilisateur dans l'Active Directory	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	PC personnel + Téléphone personnel	

1.2 Des outils sont mobilisés pour la gestion de la sécurité :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Gestion des incidents	GLPI pour le suivi des tickets	
Détection et prévention des intrusions	Port security	
Chiffrement	VPN IPSec (AES-256) entre les deux sites	
Analyse de trafic	Wireshark	

Rappel : les logiciels de simulation ou d'émulation sont utilisés en réponse à des besoins de l'organisation. Ils ne peuvent se substituer complètement à des équipements réels dans l'environnement technologique d'apprentissage.

(suite) ANNEXE VII-7 : Modèle d'attestation de respect de l'annexe II.E « Environnement technologique pour la certification » du référentiel

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

2. Éléments spécifiques à l'option « Solutions d'infrastructure, systèmes et réseaux » (SISR)

Rappel de l'annexe II.E du référentiel : **« *Une solution d'infrastructure réduite à une simulation par un logiciel ne peut être acceptée.* »**

2.1 L'environnement technologique supportant le système d'information de l'organisation cliente comporte au moins :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Un réseau comportant plusieurs périmètres de sécurité	Isolation par des VLAN en fonctionne des types de machines connecté (Serveur, Client, Wifi…)	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Serveur Web avec HA	
Un logiciel d'analyse de trames	Wireshark sur le Bastion	
Un logiciel de gestion des configurations	GPO	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	SSH/RDP	
Une solution permettant la supervision de la qualité, de la sécurité et de la disponibilité des équipements d'interconnexion, serveurs, systèmes et services avec remontées d'alertes	Zabbix	
Une solution garantissant des accès sécurisés à un service, internes au périmètre de sécurité de l'organisation (type intranet) ou externes (type internet ou extranet)	VPN	
Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution garantissant la continuité d'un service	HA Proxy + redondance switch + routeurs en HA	

Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Routeurs en HA et redondance switch	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HA Proxy + routeurs en HA et redondance switch	

2.2 La structure et les activités de l'organisation s'appuient sur au moins une solution d'infrastructure opérationnelle parmi les suivantes :

Éléments	**Description de l'implantation dans le centre d'examen (nom du service ou de l'outil et caractéristiques techniques)**	**Remarques de la commission d'interrogation**
Une solution permettant la connexion sécurisée entre deux sites distants	VPN IPSec entre les deux firewall distant (Fortigate / PFSense)	
Une solution permettant le déploiement des solutions techniques d'accès	GPO de l'Active Directory	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	Script PowerShell pour la création et l'intégration des utilisateurs dans l'AD	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Port security et Zabbix	