PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : Gobert

Prénom : Pierre-Louis

Établissement de formation (sur un seul des deux exemplaires du dossier)

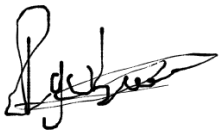
Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

Nom et qualité du signataire	Date	Signature
BOLLIN Antonin Formateur SIO SISR	23/04/2026	

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), Gobert , Pierre-Louis , certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à La Roche sur yon
Date 24/04/2026 **Signature**



Sommaire

GOBERT PIERRE-LOUIS BTS
SIO - OPTION A - SISR
CANDIDAT N°02046022493
SESSION 2026

1. Présentation du projet Orion

L’entreprise pédagogique Oasis est une société parisienne spécialisée dans le voyage sur mesure.

Créée en 2017, elle s’appuie sur une forte personnalisation de ses services et sur un réseau de partenaires dans plus de 30 pays. En 2024, son chiffre d’affaires atteint 2,3 millions d’euros.

L’entreprise est organisée autour de plusieurs services métiers et utilise au quotidien des outils collaboratifs, une messagerie professionnelle, un cloud interne et des postes clients sous Windows 10/11.

Avec l’ouverture d’une agence à Marseille en complément du siège de Paris, Oasis doit moderniser son infrastructure afin de sécuriser les échanges, centraliser les services et améliorer la communication inter-sites.

2. Contexte et problématique

L’entreprise pédagogique Oasis connaît une phase de croissance avec un siège à Paris et une agence récemment ouverte à Marseille.

Les équipes utilisent quotidiennement des outils collaboratifs, des services internes et des postes de travail connectés au système d’information.

Cette évolution impose une infrastructure plus structurée, capable de centraliser les échanges, sécuriser les données et faciliter le travail entre les deux sites.

Dans un premier temps, l’agence de Marseille devait disposer d’une infrastructure locale fonctionnelle, sécurisée et évolutive, tout en restant prête à être raccordée au siège.
Le réseau devait donc être administrable, segmenté et suffisamment robuste pour accueillir les services et les utilisateurs de l’agence dans de bonnes conditions.

La problématique principale du projet était ensuite de permettre une communication sécurisée entre Paris et Marseille, sans exposer les flux sensibles sur le réseau WAN. Il fallait donc définir un plan d’adressage cohérent, configurer les équipements de bordure, chiffrer les échanges inter-sites et filtrer uniquement les flux nécessaires.

Dans ce cadre, les solutions retenues ont porté sur :

- la mise en place d’un pare-feu Stormshield pour sécuriser l’interconnexion entre les deux sites ;
- la configuration d’un switch Cisco pour assurer la segmentation en VLAN, le transport des flux réseau et l’administration du LAN.

3. Vue d’ensemble de l’infrastructure

L’infrastructure du projet Orion repose sur une architecture multi-sites composée d’un site principal à Paris et d’un site distant à Marseille.

Le site de Paris héberge plusieurs services centraux virtualisés, tandis que le site de Marseille dispose d’une infrastructure locale physique et virtualisée permettant d’accueillir les utilisateurs et les services de proximité.

La communication entre les deux sites est assurée par un tunnel VPN IPsec mis en place entre les équipements de sécurité.

À Marseille, le pare-feu Stormshield protège le réseau local et gère l’interconnexion avec le site distant. Le switch Cisco permet quant à lui d’organiser le réseau local en plusieurs VLAN, afin de séparer les usages, sécuriser les flux et faciliter l’administration.

Cette architecture permet de répondre aux besoins de l’entreprise en matière de segmentation réseau, de sécurisation des échanges et de continuité de service entre les deux sites.

3. VUE D'ENSEMBLE DE L'INFRASTRUCTURE (TOPOLOGIE PHYSIQUE)

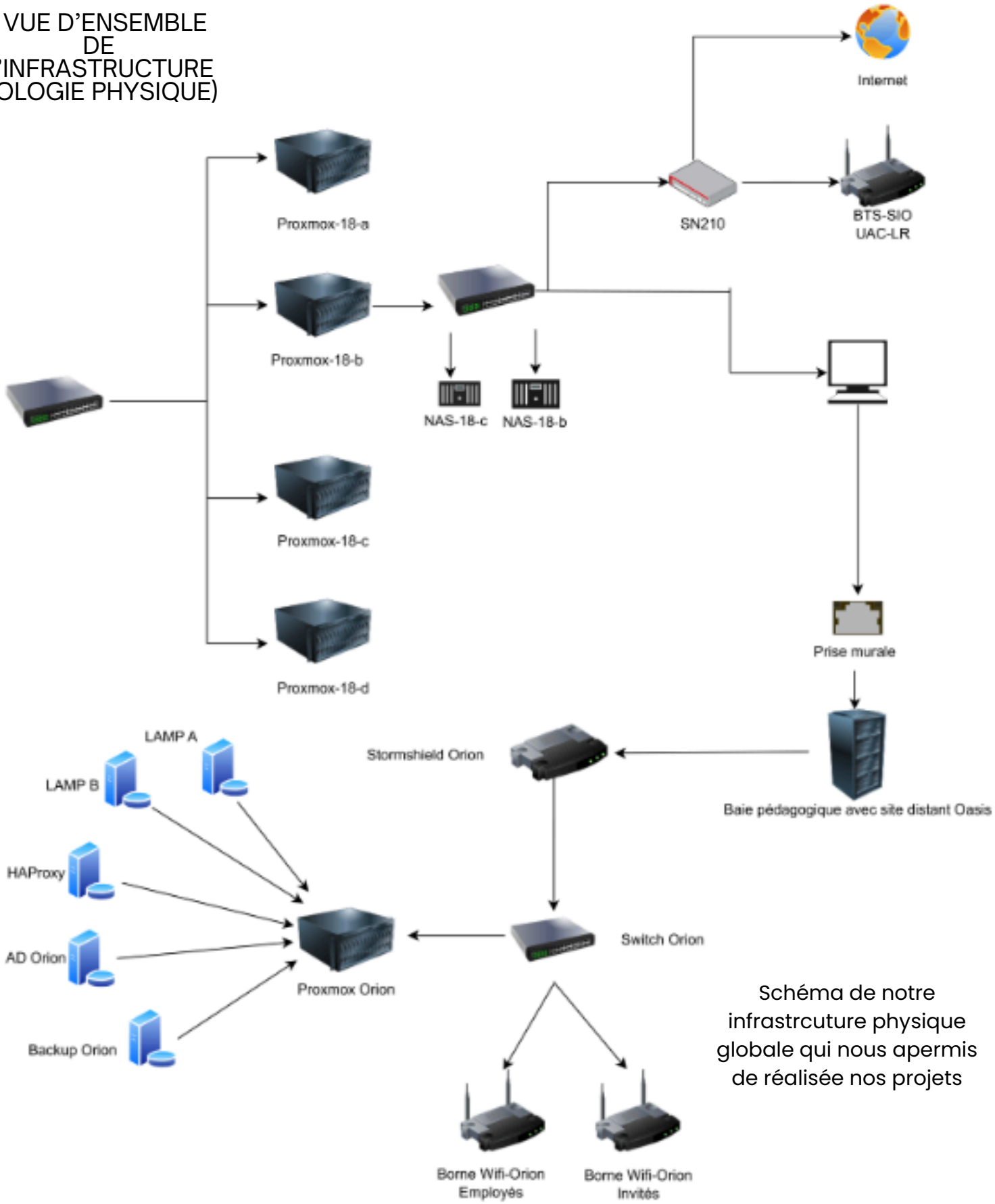
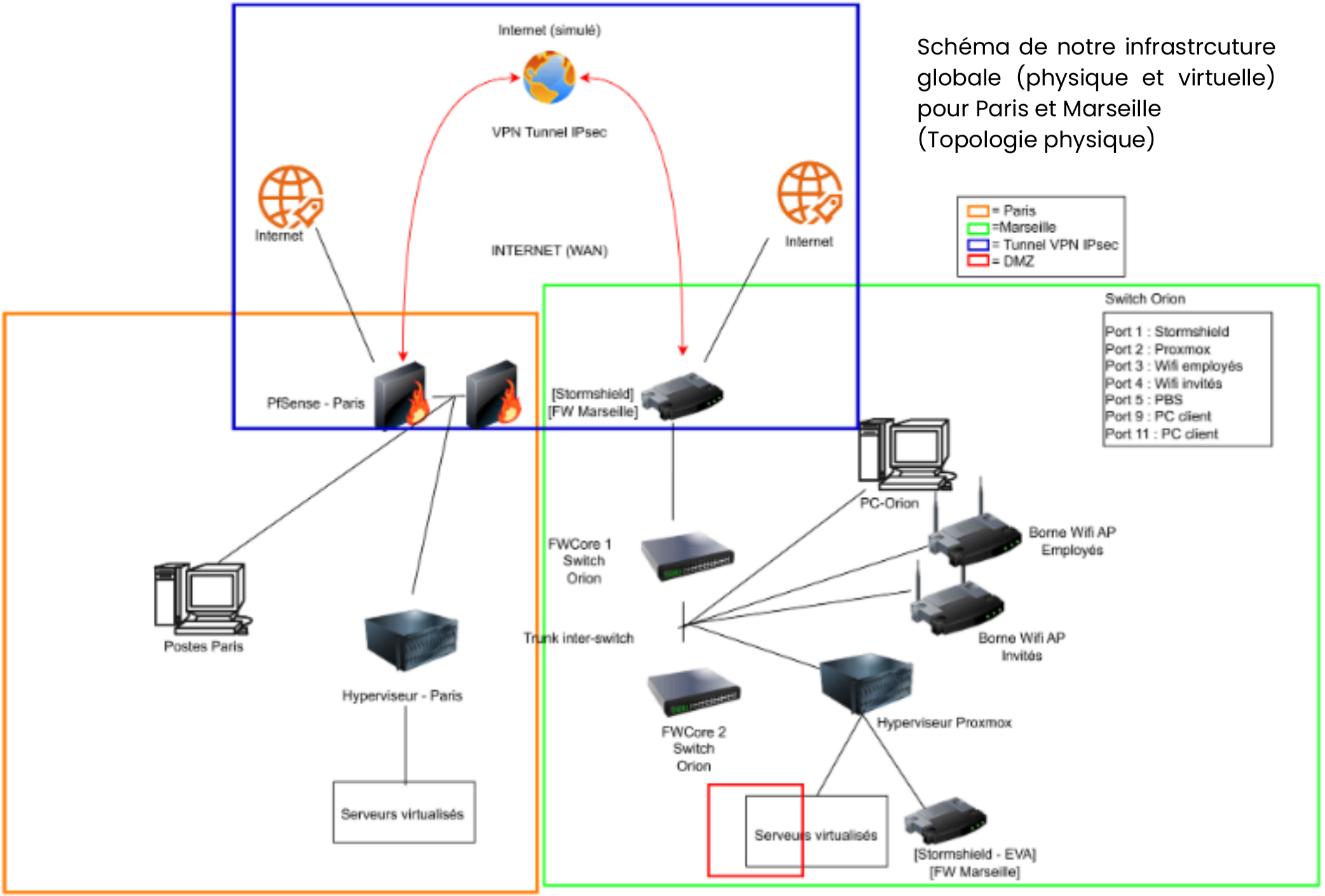
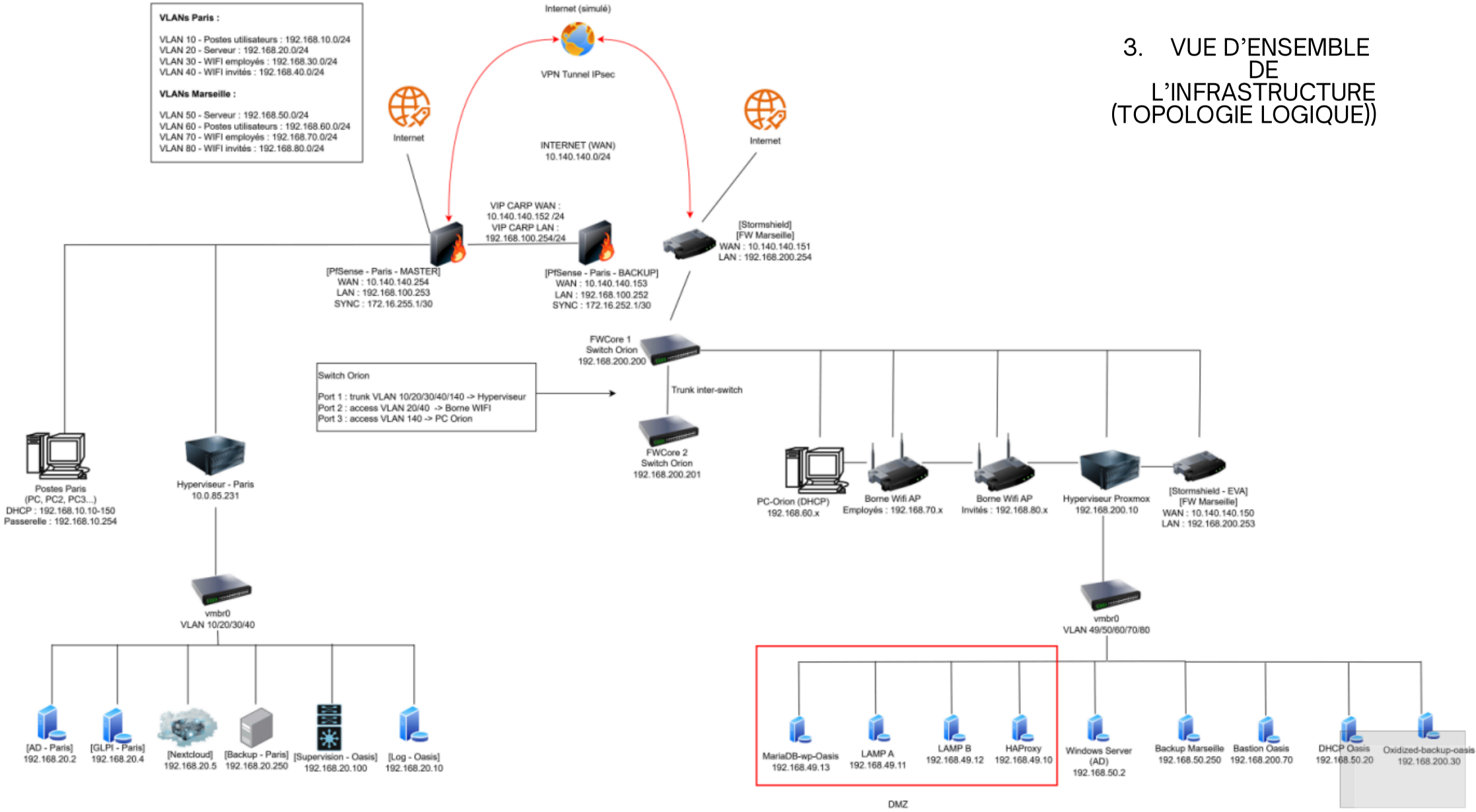


Schéma de notre infrastrcuture physique globale qui nous apermis de réalisée nos projets

Schéma de notre infrastrcuture globale (physique et virtuelle) pour Paris et Marseille (Topologie physique)



3. VUE D'ENSEMBLE DE L'INFRASTRUCTURE (TOPOLOGIE LOGIQUE))



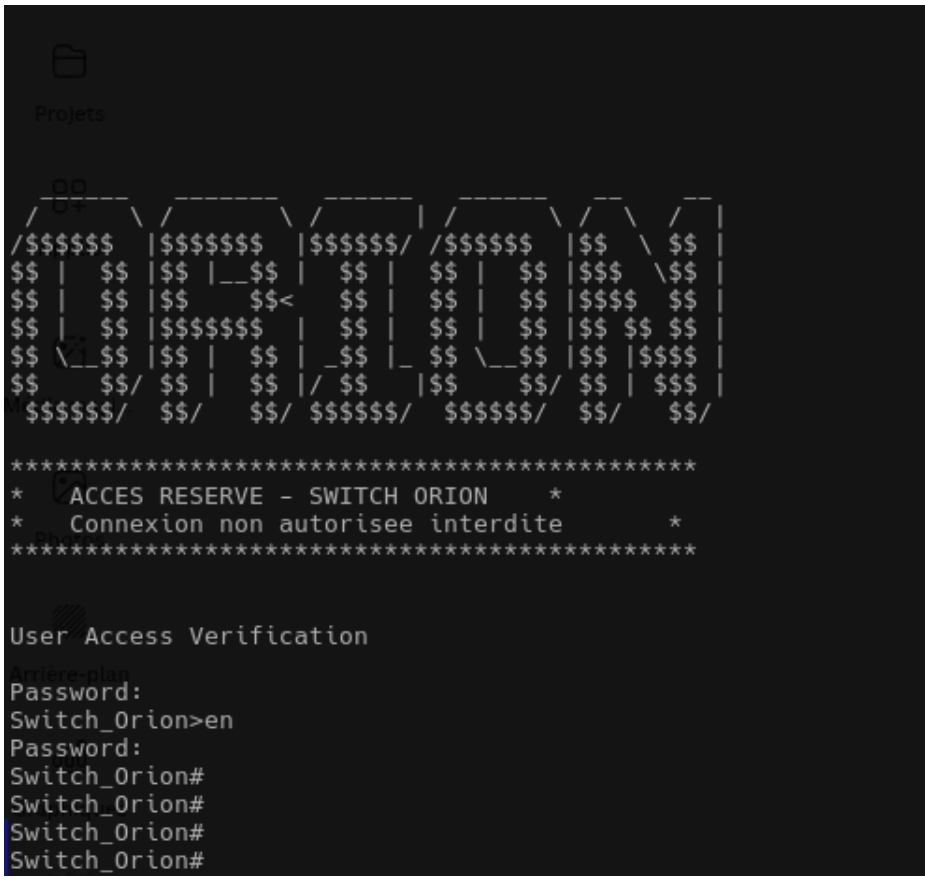
4. Solution 2 : Configuration du switch Cisco

Le switch Cisco a été configuré sur le site de Marseille afin d'organiser le réseau local et de transporter les différents VLAN vers les équipements principaux de l'infrastructure.

Son rôle est de connecter les postes clients, les serveurs, les bornes Wi-Fi, le pare-feu Stormshield et l'hyperviseur Proxmox, tout en séparant les usages réseau.

La configuration réalisée repose sur :

- la création des VLAN ;
- la configuration des ports en access ou en trunk ;
- le transport des VLAN vers le Stormshield, Proxmox et les bornes Wi-Fi ;
- l'administration du switch via un réseau dédié.



4. Solution 2 : Configuration du switch Cisco

Le switch Cisco a été configuré afin de segmenter le réseau local de Marseille en plusieurs VLAN.

La commande show vlan brief permet de vérifier la présence des VLAN et l'affectation des ports :

- VLAN 49 : DMZ Web
- VLAN 50 : Serveurs
- VLAN 60 : Utilisateurs
- VLAN 70 : Wi-Fi employés
- VLAN 80 : Wi-Fi invités
- VLAN 140 : WAN
- VLAN 200 : Management

Cette segmentation permet de séparer les usages réseau, de sécuriser les flux et de faciliter l'administration.

```
Switch_Orion#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/12
49   DMZ_WEB                          active
50   SERVERS                          active    Gi1/0/5
60   USERS                            active    Gi1/0/6, Gi1/0/7, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
70   WIFI_EMPLOYES                    active    Gi1/0/3
80   WIFI_INVITES                     active    Gi1/0/4
140  WAN                              active    Gi1/0/25, Gi1/0/26, Gi1/0/27
                                                Gi1/0/28
200  MGMT                             active    Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

5. Tests et validation de la solution Switch Cisco

Test 1 — Vérification des VLAN

La commande show vlan brief permet de confirmer que les VLAN nécessaires sont bien créés et actifs sur le switch.
Elle valide aussi l'affectation des ports access aux bons réseaux, comme les VLAN 50 Serveurs, 60 Utilisateurs, 70 Wi-Fi employés, 80 Wi-Fi invités et 200 Management.

Test 2 — Vérification des trunks

La commande show interfaces trunk confirme que les liens trunk sont actifs et qu'ils transportent les VLAN nécessaires vers les équipements principaux, notamment le Stormshield, Proxmox et le lien d'agrégation Po1.
Bilan
Les tests réalisés confirment que le switch assure correctement la segmentation réseau et le transport des VLAN entre les équipements de l'infrastructure.

Test de connectivité

Un test de connectivité a été réalisé depuis l'hyperviseur Proxmox Orion.
Le ping vers 192.168.200.200 permet de vérifier la communication avec le switch.
Le ping vers 8.8.8.8 confirme que la sortie Internet est fonctionnelle via le switch Cisco et le pare-feu.

```
root@proxmox-orion:~# ping -c 2 192.168.200.200
PING 192.168.200.200 (192.168.200.200) 56(84) bytes of data.
64 bytes from 192.168.200.200: icmp_seq=1 ttl=255 time=1.23 ms
64 bytes from 192.168.200.200: icmp_seq=2 ttl=255 time=1.55 ms

--- 192.168.200.200 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 1.233/1.389/1.546/0.156 ms
root@proxmox-orion:~# ping -c 2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=9.29 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=8.87 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 8.870/9.080/9.290/0.210 ms
```

6. Conclusion

La configuration du switch Cisco a permis de structurer le réseau local de Marseille grâce à la mise en place de plusieurs VLAN.

Les ports ont été configurés selon leur usage : en trunk pour transporter plusieurs VLAN vers les équipements principaux comme le Stormshield et Proxmox, et en access pour les équipements associés à un seul réseau.

Cette configuration permet de séparer les usages réseau, notamment les serveurs, les utilisateurs, le Wi-Fi, la DMZ, le WAN et le management.

Les tests réalisés confirment que les VLAN sont actifs, que les trunks transportent correctement les réseaux nécessaires et que l'infrastructure dispose bien d'une connectivité réseau fonctionnelle.

Le switch Cisco assure donc correctement son rôle de distribution, de segmentation et d'acheminement des flux dans l'infrastructure Orion.

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]		**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 sous Windows Server 2022 virtualisé sur Proxmox VE, avec gestion centralisée des utilisateurs, groupes, unités d'organisation, stratégies de groupe (GPO), authentification sur les postes clients et réplication inter-sites Paris / Marseille.	
Un SGBD	MariaDB / MySQL sous Debian 12, déployé sur machine virtuelle dédiée, utilisé pour les services applicatifs internes tels que GLPI, Centreon et certaines applications web de l'infrastructure.	
Un accès sécurisé à internet	Pare-feu pfSense virtualisé pour le site de Paris et pare-feu Stormshield pour le site de Marseille, assurant le filtrage des flux, le NAT, le routage inter-VLAN, la publication contrôlée des services et l'interconnexion sécurisée des sites via VPN IPsec.	
Un environnement de travail collaboratif	Nextcloud pour le partage, la synchronisation et l'accès distant aux documents de l'entreprise, complété par des partages SMB / Windows sécurisés et intégrés à l'annuaire Active Directory pour la gestion des droits d'accès.	

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

Deux serveurs, éventuellement virtualisés, basés sur des systèmes d'exploitation différents, dont l'un est un logiciel libre (*open source)*	Infrastructure mixte reposant sur des serveurs virtualisés sous Proxmox VE : • Windows Server pour les services d'annuaire, DNS, GPO et administration Windows • Debian pour les services applicatifs, web, supervision, sauvegarde et collaboration	

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) dédié à la sauvegarde des machines virtuelles et conteneurs, avec planification automatisée, politique de rétention, journalisation des tâches et tests de restauration partielle et complète.	
Des ressources dont l'accès est sécurisé et soumis à habilitation	Contrôle d'accès basé sur Active Directory, groupes de sécurité, droits NTFS / partages réseau, règles de filtrage pare-feu, segmentation VLAN et restriction des accès d'administration aux seuls comptes habilités.	
Deux types de terminaux dont un mobile (type *smartphone* ou encore tablette)	Postes clients Windows 10 / Windows 11 intégrés au domaine, ainsi que terminaux mobiles ou tablettes connectés au réseau Wi-Fi invité ou au réseau interne selon les profils d'accès définis.	

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 la gestion de parc, l'inventaire matériel / logiciel, le suivi des incidents, la traçabilité des interventions et la centralisation du support informatique.	
Détection et prévention des intrusions	Fonctions de filtrage et de sécurité assurées par pfSense et Stormshield avec fonctions IDS/IPS activées et Stormshield avec règles de sécurité avancées, avec contrôle des flux inter-sites et inter-VLAN, limitation des accès non autorisés et surveillance des comportements réseau anormaux.	
Chiffrement	Chiffrement des communications via VPN IPsec entre Paris et Marseille, services web sécurisés en HTTPS / TLS, authentification chiffrée sur les services internes et sécurisation des accès Wi-Fi par WPA2/WPA3 selon les usages.	
Analyse de trafic	Analyse des journaux et des flux réseau via Graylog / centralisation des logs, complétée par l'utilisation d'outils d'analyse de paquets et de supervision pour l'investigation et le diagnostic réseau.	

(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	Infrastructure réseau segmentée en plusieurs VLAN selon les usages et niveaux de sensibilité : utilisateurs, serveurs, administration, Wi-Fi employés, Wi-Fi invités, avec filtrage inter-VLAN et sécurisation des échanges entre le siège de Paris et l'agence de Marseille.	
Un service rendu à l'utilisateur final respectant un contrat de service comportant des contraintes en termes de sécurité et de haute disponibilité	Services utilisateurs sécurisés et supervisés (authentification, partage documentaire, applications web internes, accès inter-sites), avec sauvegarde régulière, supervision centralisée, contrôle des accès et mécanismes de continuité de service adaptés à la maquette.	
Un logiciel d'analyse de trames	Wireshark, utilisé pour l'analyse de trames, le diagnostic des communications réseau, la vérification des échanges entre VLAN, le contrôle des flux applicatifs et les tests de connectivité inter-sites.	
Un logiciel de gestion des configurations	Sauvegarde et centralisation des configurations techniques des équipements et services (pare-feux, switchs, machines virtuelles, services), avec conservation sécurisée des identifiants et secrets dans KeePass.	
Une solution permettant l'administration à distance sécurisée de serveurs et de solutions techniques d'accès	Administration sécurisée à distance via SSH, RDP, interfaces web d'administration en HTTPS, accès restreints par VLAN d'administration et, selon le besoin, transit via le VPN inter-sites pour les opérations techniques.	
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	Centreon déployé sur serveur dédié pour superviser les serveurs, services, équipements réseau et disponibilités inter-sites, avec tableaux de bord, seuils d'alerte, remontées d'événements et historisation des performances.	

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)	Accès sécurisés aux services internes et externes via authentification Active Directory, chiffrement HTTPS / TLS, segmentation réseau, filtrage pare-feu et VPN IPsec pour les échanges entre les deux sites.	
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	Sauvegardes automatisées, procédures de restauration testées, plan de reprise d'activité simplifié et architecture inter-sites permettant le maintien ou la reprise rapide des services critiques en cas d'incident.	
Une solution garantissant la tolérance de panne de systèmes serveurs ou d'éléments d'interconnexion	Tolérance de panne assurée par la virtualisation des services, la sauvegarde des machines et configurations, l'interconnexion entre les sites et la présence d'équipements réseau redondés sur la maquette selon les scénarios déployés.	
Une solution permettant la répartition de charges entre services, serveurs ou éléments d'interconnexion	HAProxy utilisé pour la répartition de charge des services web internes, avec distribution des requêtes entre plusieurs serveurs applicatifs afin d'améliorer la disponibilité et la continuité du service.	

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	Tunnel VPN IPsec site-à-site entre le pare-feu pfSense du siège de Paris et le pare-feu Stormshield de l'agence de Marseille, permettant l'échange sécurisé des flux réseau entre les deux infrastructures.	
Une solution permettant le déploiement des solutions techniques d'accès	Déploiement des postes et services d'accès via DHCP, intégration au domaine Active Directory, résolution DNS interne, application de stratégies de groupe (GPO) et gestion centralisée des comptes utilisateurs.	
Une solution gérée à l'aide de procédures automatisées écrites avec un langage de *scripting*	Automatisation de certaines tâches d'administration à l'aide de scripts PowerShell et de tâches planifiées, ainsi que d'outils natifs Linux (bash / cron) pour les opérations de maintenance, de supervision ou de sauvegarde.	
Une solution permettant la détection d'intrusions ou de comportements anormaux sur le réseau	Détection des comportements anormaux via la corrélation des journaux, la supervision Centreon, l'analyse centralisée des logs et les mécanismes de sécurité des pare-feux déployés sur les 2 sites.	

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 :**
Nom, prénom :Gobert Pierre-Louis	**N° candidat : 02046022493**
Épreuve ponctuelle ☒ **Contrôle en cours de formation** ☐	**Date : 09** / 06 / 2026

Organisation support de la réalisation professionnelle

Entreprise Oasis (maquette pédagogique)
Entreprise spécialisée dans les voyages sur mesure avec un siège à Paris et une agence à Marseille

Intitulé de la réalisation professionnelle

Mise en place d'une infrastructure réseau sécurisée et segmentée pour l'agence Oasis Marseille avec interconnexion au siège de Paris

Période de réalisation : 2024-2026 **Lieu :** 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)

La réalisation s'inscrit dans le cadre du projet Oasis visant à déployer une infrastructure complète pour l'agence de Marseille, puis à l'interconnecter de manière sécurisée avec le siège de Paris.

Les objectifs étaient :

- mettre en place un réseau local fonctionnel et sécurisé ;
- segmenter le réseau en VLAN selon les usages ;
- sécuriser les flux via un pare-feu ;
- assurer une communication inter-sites sécurisée.

Le travail a été réalisé dans un environnement de test virtualisé sous **Proxmox**, reproduisant une infrastructure réelle.

[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]

Matériel / Virtualisation

- Proxmox (hyperviseur)
- Switch Cisco
- Pare-feu Stormshield
- Postes clients et VM

Logiciels / Services

- pfSense (Paris)
- Stormshield (Marseille)
- Linux / Windows Server
- DNS, DHCP, AD

Outils

- CLI Cisco
- Interface Stormshield
- Ping / Test-NetConnection
- Navigateur web

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

Les productions sont accessibles via :

- l'environnement Proxmox (machines virtuelles)
- les interfaces web des équipements (Stormshield, services)
- les configurations réseau (switch, firewall)
- les captures d'écran du dossier

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)

[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.

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

Dans le cadre du projet Oasis, une infrastructure réseau a été conçue et déployée pour l'agence de Marseille, avec pour objectif de créer un environnement sécurisé, structuré et interconnecté avec le siège de Paris.

Deux solutions principales ont été mises en place :

1. Mise en place du pare-feu Stormshield

Le pare-feu Stormshield a été déployé afin de sécuriser le réseau local et de permettre l'interconnexion avec le site de Paris.

Un tunnel **VPN IPsec** a été configuré pour chiffrer les communications entre les deux sites, garantissant la confidentialité des échanges.

Une **politique de filtrage** a également été mise en place, organisée par blocs, afin de contrôler les flux réseau :

- accès internes selon les profils (utilisateurs, serveurs, invités) ;
- accès d'administration via un réseau dédié ;
- flux inter-sites via le VPN ;
- blocage des communications non autorisées.

Des tests ont permis de valider :

- l'établissement du tunnel VPN ;
- la communication entre les deux sites ;
- le respect des règles de filtrage.

2. Configuration du switch Cisco

Le switch Cisco a été configuré afin d'assurer la **segmentation du réseau local** grâce à la mise en place de plusieurs VLAN.

Les VLAN permettent de séparer les usages :

- serveurs ;
- utilisateurs ;
- Wi-Fi employés ;
- Wi-Fi invités ;
- management ;
- WAN.

Les ports ont été configurés selon leur rôle :

- en **trunk** pour transporter plusieurs VLAN vers le Stormshield et Proxmox ;
- en **access** pour les équipements associés à un seul réseau.

Des tests ont été réalisés afin de vérifier :

- la présence des VLAN ;
- le bon fonctionnement des trunks ;
- la connectivité réseau interne ;
- l'accès à Internet depuis les machines.

Résultats obtenus

La mise en place de ces solutions a permis :

- une segmentation claire du réseau ;
- une sécurisation des communications inter-sites ;
- une meilleure organisation de l'infrastructure ;
- une connectivité complète entre les équipements et vers Internet.

L'infrastructure est fonctionnelle, sécurisée et évolutive, répondant aux besoins du projet Oasis.