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), Nom , Prénom , 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
Date

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)

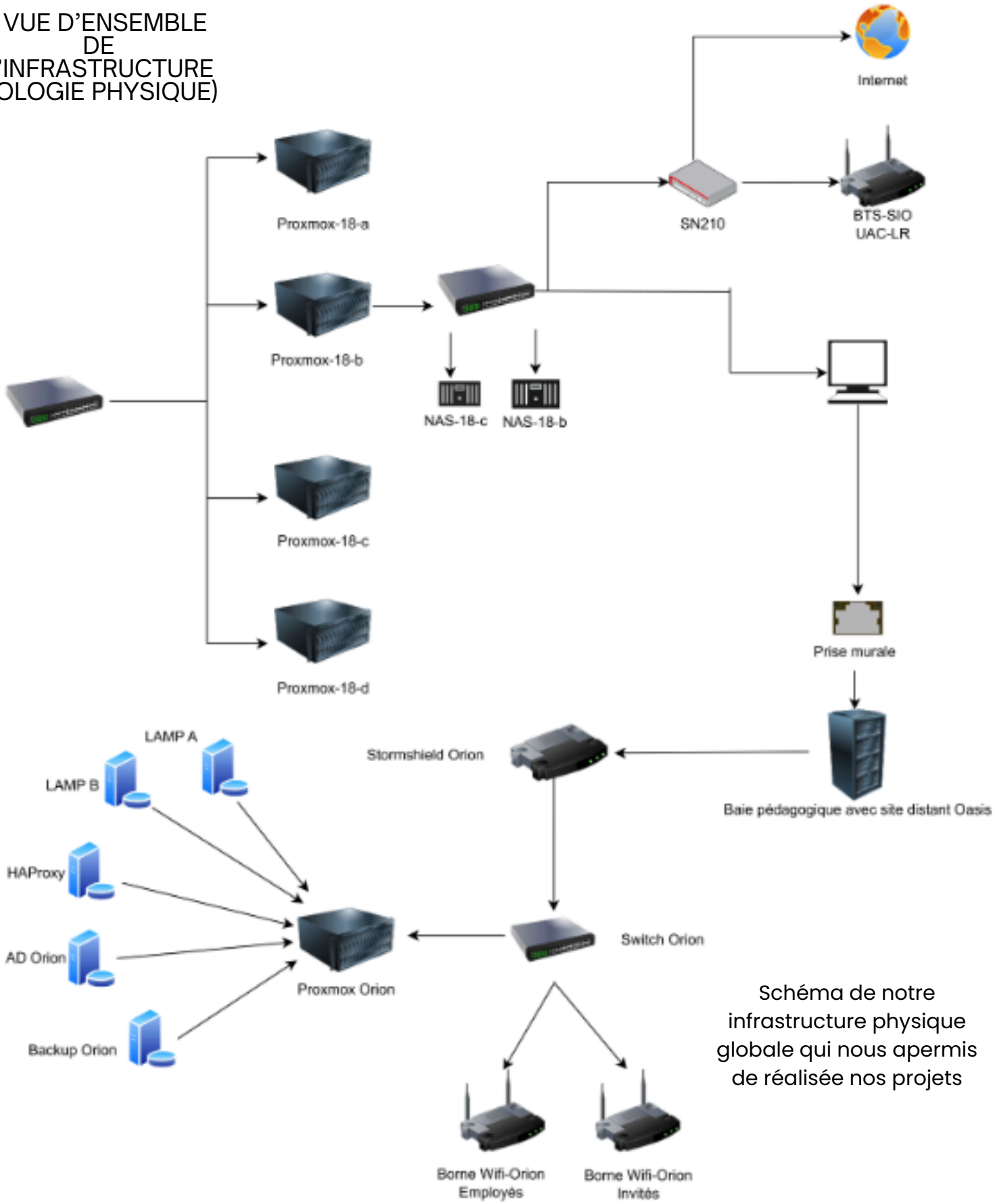
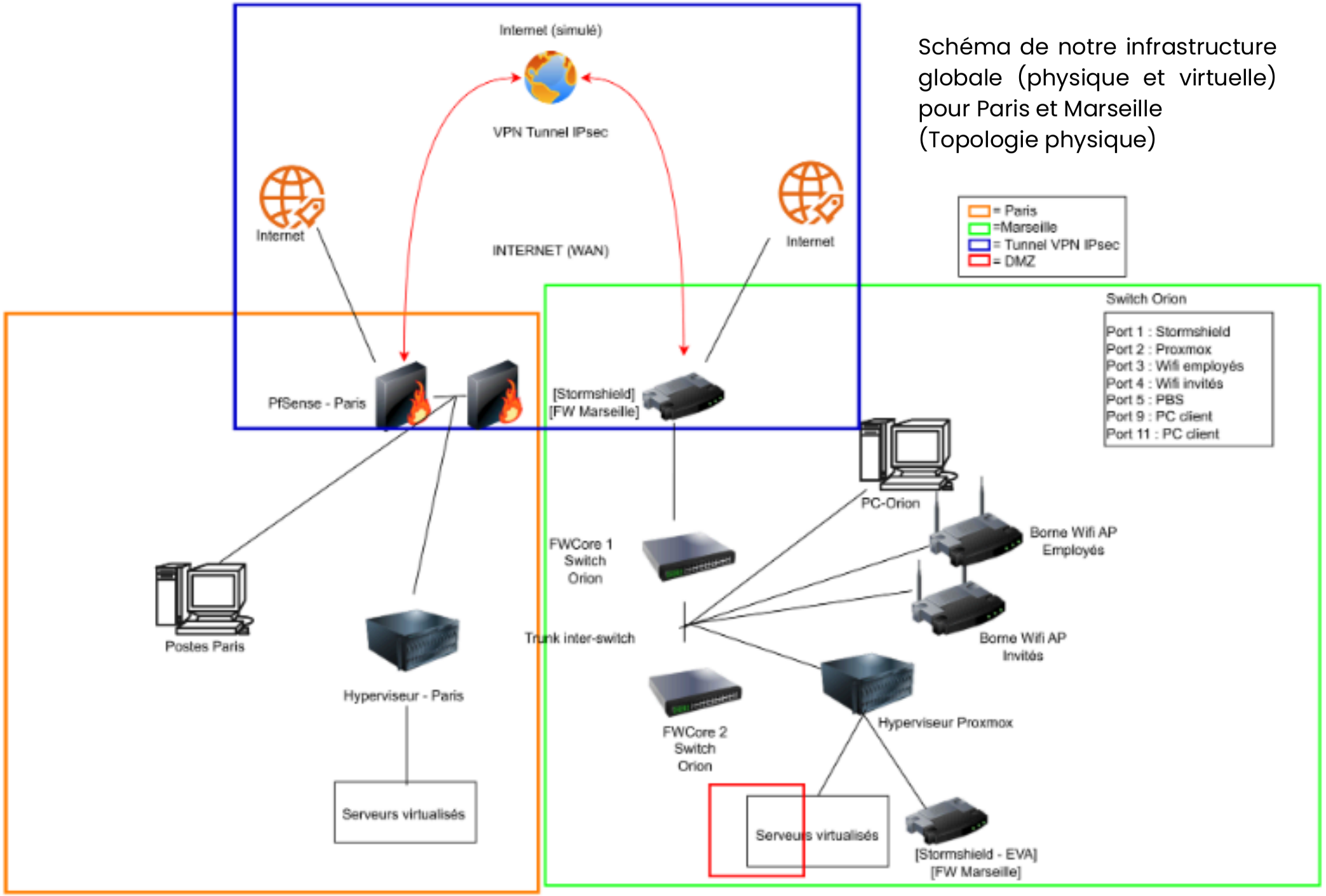
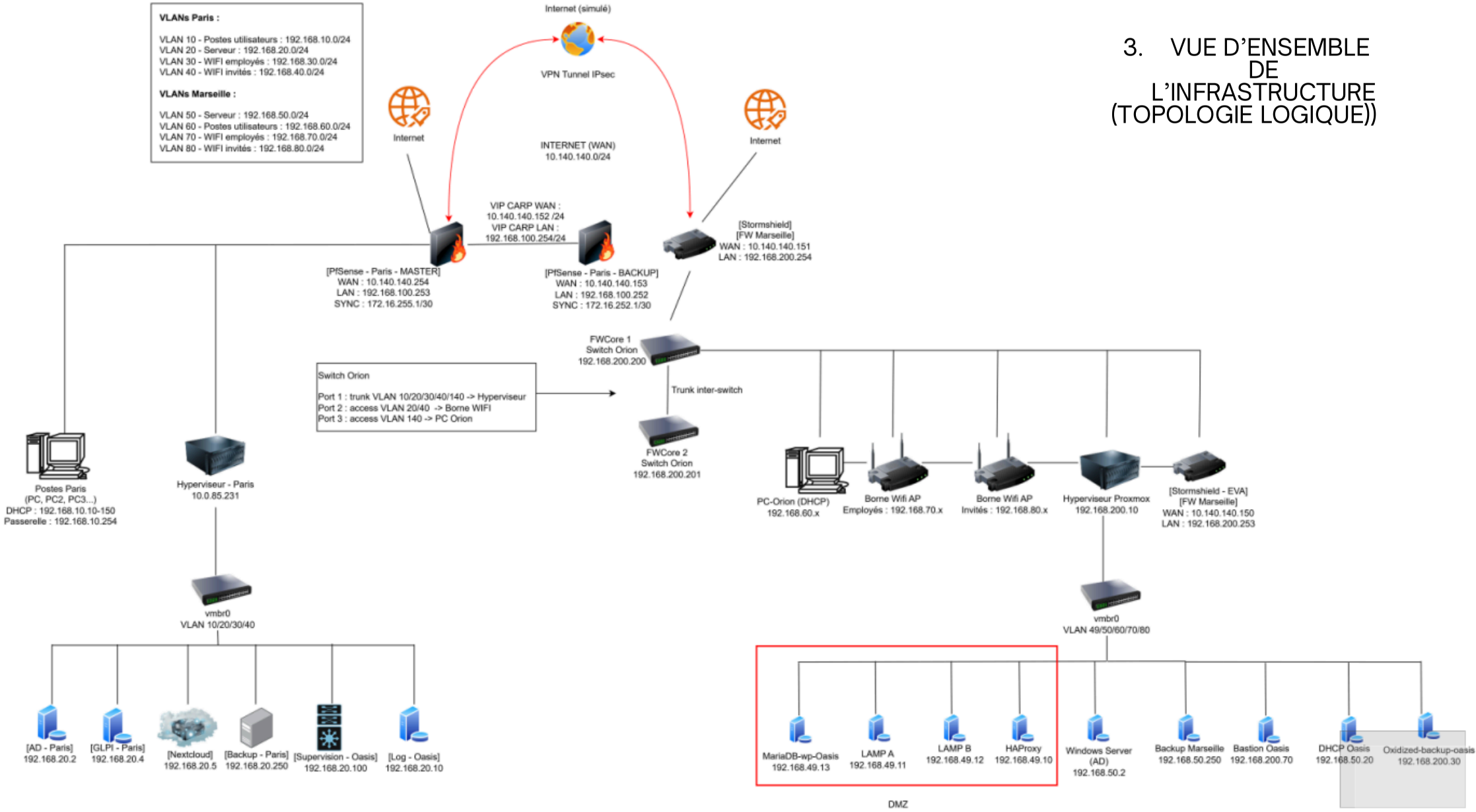


Schéma de notre infrastructure physique globale qui nous apermis de réalisée nos projets

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



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

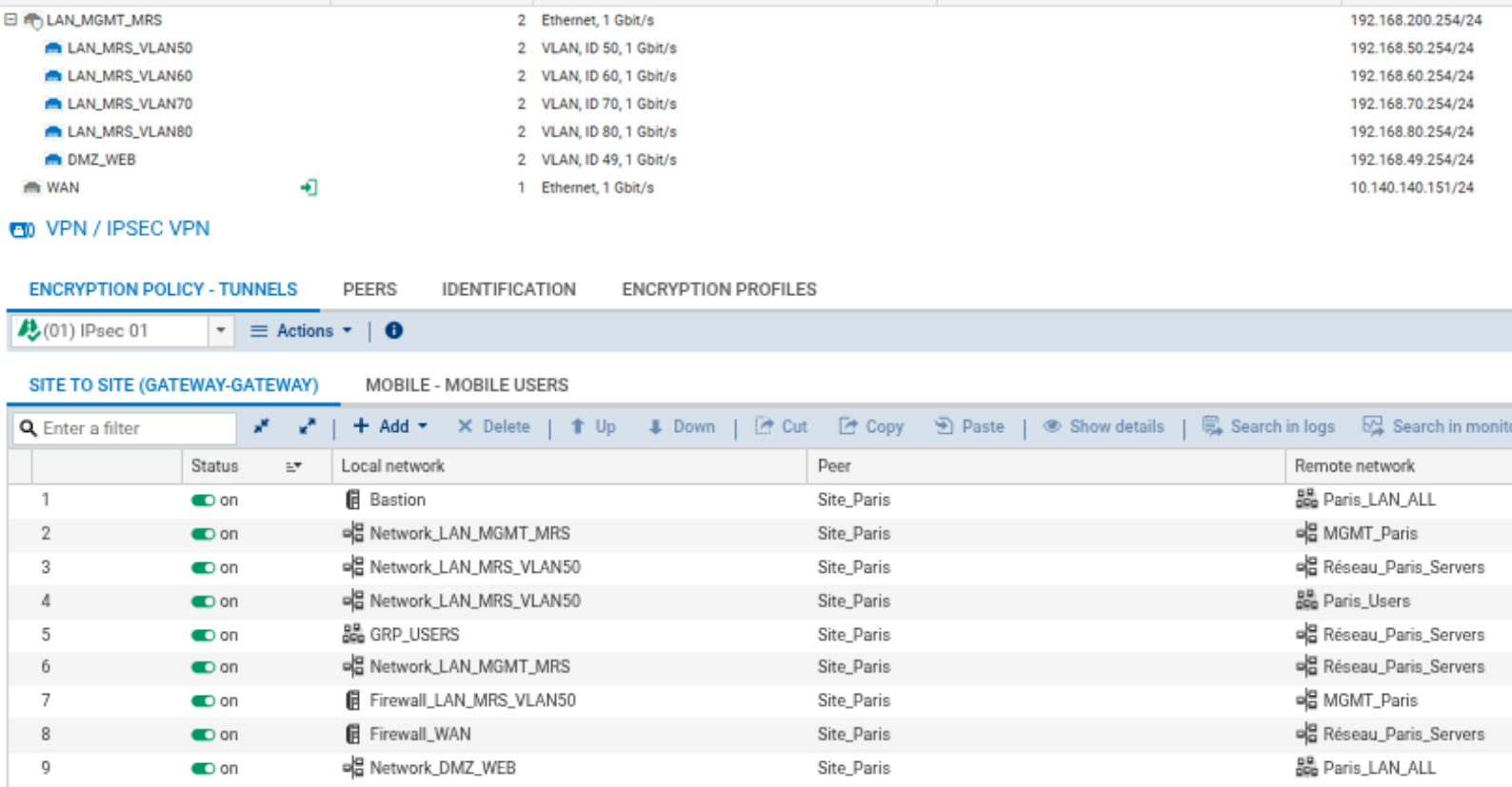


4. Solution 1 : Mise en place du pare-feu Stormshield

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

Son rôle principal est de séparer les zones réseau, de filtrer les flux et de mettre en place un tunnel VPN IPsec permettant la communication sécurisée entre les deux sites.

La configuration a porté sur les interfaces réseau, la définition des objets et sous-réseaux, la mise en place du VPN IPsec ainsi que sur les règles de filtrage autorisant uniquement les flux nécessaires.



4. Solution 1 : Mise en place du pare-feu Stormshield

La sécurisation repose sur une segmentation par blocs fonctionnels, permettant un contrôle granulaire des flux entre Marseille, la DMZ et Paris :
Bloc 0 (Firewall) : Gestion des flux internes essentiels (DNS, NTP) pour les différents profils (utilisateurs, serveurs, invités).
Bloc 1 (Bastion) : Contrôle des accès d'administration sécurisés (SSH, Web) vers les réseaux de Marseille et Paris.
Bloc 2 (DMZ Web) : Isolation des services publics (Web, SQL) et restriction des communications vers Internet ou les réseaux internes.

Bloc 0 – Firewall (contains 4 rules, from 3 to 6)							
3		on	pass	GRP_MGMT	Firewall_LAN_MGMT_MRS	SRV_WEB SRV_DNS	IPS
4		on	pass	GRP_USERS	Firewall_LAN_MRS_VLAN60 Firewall_LAN_MRS_VLAN70	SRV_DNS	IPS
5		on	pass	GRPS_SERVERS	Firewall_LAN_MRS_VLAN50	SRV_DNS SRV_NTP	IPS
6		on	pass	GRP_INVITES	Firewall_LAN_MRS_VLAN80	SRV_DNS	IPS
Bloc 1 – Bastion (contains 2 rules, from 7 to 8)							
7		on	pass	Bastion	Grp_LAN_MRS Paris_LAN_ALL	Any	FW
8		on	pass	Bastion	Internet	Any	IPS
Bloc 2 – DMZ WEB (contains 7 rules, from 9 to 15)							
9		on	pass	GRP_DMZ	Firewall_DMZ_WEB	Any	IPS
10		on	pass	Ha_Proxy	GRP_LAMP	SRV_WEB	IPS
11		on	pass	Network_DMZ_WEB	Internet	SRV_NTP SRV_WEB SRV_DNS	IPS
12		on	pass	GRP_LAMP	MariaDB	mysql	IPS
13		on	pass	Grp_LAN_MRS Paris_LAN_ALL	Ha_Proxy	SRV_WEB	IPS
14		on	block	Any	GRP_LAMP	SRV_WEB	IPS
15		on	block	Network_DMZ_WEB	Any	Any	IPS

4. Solution 1 : Mise en place du pare-feu Stormshield

La configuration se termine par la gestion de l'infrastructure locale et le verrouillage final du réseau :

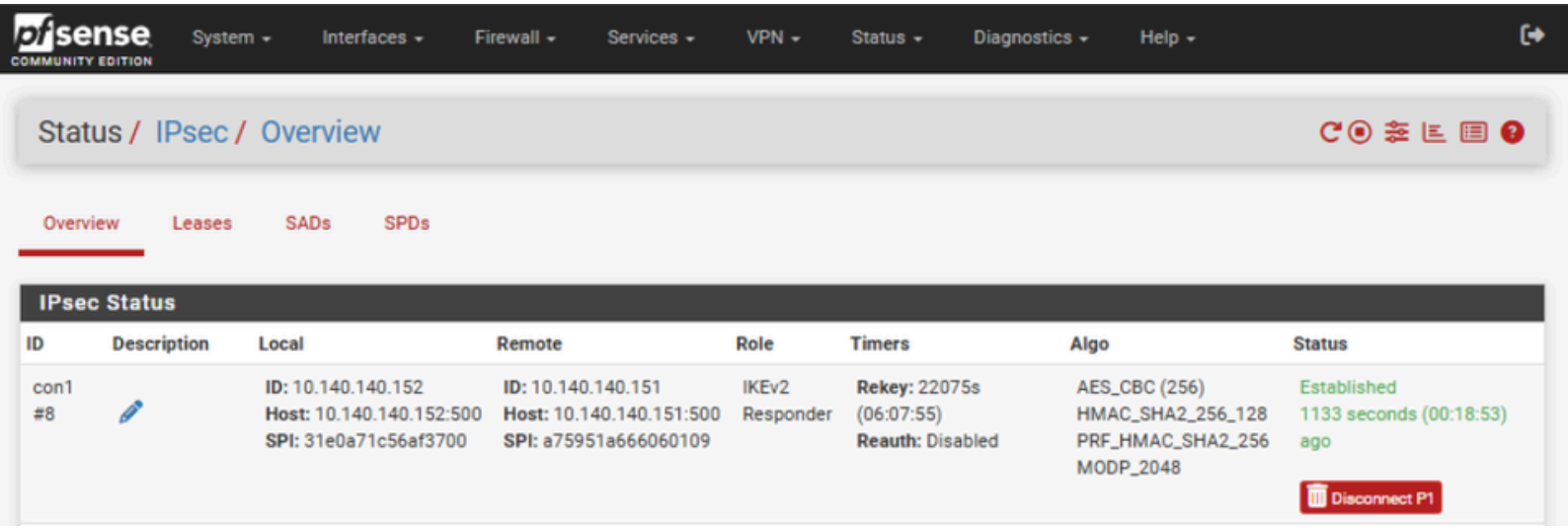
- Bloc 6 (IPsec MRS) : Interconnexion sécurisée entre Marseille et Paris, autorisant les services critiques (Active Directory, Web, Graylog) et le diagnostic ICMP.
- Bloc 7 (Infrastructure & Système) : Gestion des services de base du site (flux DHCP, synchronisation AD-MARSEILLE et AD-PARIS) et accès contrôlé des serveurs vers Internet.
- Bloc 8 (Segmentation interne) : Application du principe de "moindre privilège" avec une règle de blocage final (Any/Any), interdisant tout flux non explicitement autorisé.

Bloc 6 – IPsec MRS - PARIS (contains 7 rules, from 37 to 43)								
37		on	pass	GRPS_SERVERS	Réseau_Paris_Servers	SRV_AD_CORE SRV_WEB SRV_NTP SRV_DNS		FW
38		on	pass	Réseau_Paris_Servers	GRPS_SERVERS	SRV_AD_CORE SRV_WEB SRV_AD_Users SRV_NTP		FW
39		on	pass	Réseau_Paris_Servers	GRP_USERS	SRV_AD_Users SRV_WEB		FW
40		on	pass	DHCP_SERVER	Grp_LAN_MRS	dhcp-boots		FW
41		on	pass	Firewall_LAN_MRS_VLAN50	DHCP_SERVER	dhcp-boots		FW
42		on	pass	GRP_MGMT GRPS_SERVERS GRP_USERS Paris_LAN_ALL	Réseau_Paris_Servers Grp_LAN_MRS	Any	icmp	FW
43		on	block	Paris_LAN_ALL GRP_USERS GRP_INVITES GRP_DMZ	Paris_LAN_ALL Grp_LAN_MRS	Any		IPS
Bloc 7 – Infrastructure & Système Servers (contains 5 rules, from 44 to 48)								
44		on	pass	GRPS_SERVERS	SRV-AD-PARIS SRV-AD-MARSEILLE	SRV_AD_Users SRV_DNS		FW
45		on	pass	GRPS_SERVERS	Internet	SRV_NTP SRV_DNS SRV_WEB		IPS
46		on	pass	GRPS_SERVERS	Internet	Any	icmp	FW
47		on	block	GRPS_SERVERS	GRP_USERS	Any		IPS
48		on	block	GRPS_SERVERS	Any	Any		IPS
Bloc 8 – Segmentation interne Marseille (contains 1 rules, from 49 to 49)								
49		on	block	Any	Any	Any		IPS

5. Tests et validations

Vérification de l'état du tunnel VPN IPsec

L'état Established du tunnel confirme que la liaison sécurisée entre Marseille et Paris est opérationnelle et que les échanges inter-sites peuvent être réalisés à travers le VPN.




```
C:\Users\solene.rigal>ipconfig

Configuration IP de Windows


Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : oasis.local
   Adresse IPv6 de liaison locale. . . . .: fe80::5ac7:4837:3845:ecb4%9
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.60.50
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . : 192.168.60.254

C:\Users\solene.rigal>ping 192.168.20.2

Envoi d'une requête 'Ping'  192.168.20.2 avec 32 octets de données :
Réponse de 192.168.20.2 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.20.2 : octets=32 temps=2 ms TTL=127
Réponse de 192.168.20.2 : octets=32 temps=3 ms TTL=127
Réponse de 192.168.20.2 : octets=32 temps=3 ms TTL=127

Statistiques Ping pour 192.168.20.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms

C:\Users\solene.rigal>
```

Vérification de la connectivité inter-sites

Un test de communication a été réalisé depuis le site de Marseille vers un serveur du site de Paris. La réponse obtenue confirme le bon fonctionnement du tunnel VPN et la bonne circulation des flux autorisés entre les deux sites.

6. Conclusion

Ce projet a permis de mettre en place une infrastructure réseau sécurisée entre les sites de Paris et de Marseille.

La configuration du pare-feu Stormshield a assuré la protection du réseau local de Marseille, le filtrage des flux et l'interconnexion avec Paris grâce à un tunnel VPN IPsec.

La segmentation réseau, les règles de filtrage par blocs et la règle finale de blocage permettent de limiter les communications aux seuls flux nécessaires.
Les tests réalisés confirment le bon fonctionnement du tunnel VPN, avec un état Established, ainsi que la connectivité entre les deux sites.

Cette réalisation répond donc aux besoins de l'entreprise Oasis : sécuriser les échanges inter-sites, isoler les différents réseaux et garantir une communication fiable entre les services de Paris et de Marseille.

Elle constitue une base solide pour une infrastructure évolutive, administrable et conforme aux bonnes pratiques de sécurité réseau.

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.