Projet « INFRASEC »
-
BTS SIO 2025 Option SISR

Epreuve E5
-
Situation professionnelle 2

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : REINBOLD ANTENAT Robin	**N° candidat : 02149951102**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 25 / 04 /.2025

Organisation support de la réalisation professionnelle
L'objectif est de concevoir une infrastructure informatique redondante et sécurisée, capable d'assurer la continuité des services critiques (communications, accès aux outils métiers, supervision) en contexte de crise. Déploiement d'une solution intégrant VPN, téléphonie IP, messagerie interne, supervision et accès distant sécurisé. Le projet a été mené en environnement virtuel afin de valider techniquement la solution avant un éventuel déploiement réel.

Intitulé de la réalisation professionnelle
Projet « INFRASEC »

Période de réalisation :…06/01/2025 au 25/04/2025 **Lieu :** Strasbourg.....
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 mises à disposition comprennent des serveurs virtuels, des routeurs logiciels (pfSense), et des outils open source. Les résultats attendus incluent : une architecture réseau redondante, un accès distant sécurisé (VPN), la mise en place de services critiques (Active Directory, VoIP, messagerie), la supervision des équipements, et une documentation technique complète.

Description des ressources documentaires, matérielles et logicielles utilisées[2]
- Routeurs pfSense, serveurs Windows Server 2022, serveurs Debian, poste client pour tests.
- Asterisk (VoIP), Modoboa (messagerie), OpenVPN, PRTG Network Monitor, eBrigade.
- Documentation technique

Modalités d'accès aux productions[3] et à leur documentation[4]
Les productions du projet (schémas, captures, rapports) sont centralisées dans un dossier partagé structuré. L'accès peut se faire localement depuis un poste connecté au réseau virtuel, ou à distance via un espace cloud sécurisé. La documentation (guide utilisateur, fiches techniques, planning, livrables) est fournie en formats PDF et modifiable

https://robin-reinbold.fr/

[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.

[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 2025**

ANNEXE 9-1-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

Table des matières

Contexte

Le projet **INFRASEC** (Infrastructure Sécurisée pour les Situations d'Urgence) s'inscrit dans une démarche de modernisation et de sécurisation des systèmes d'information des Centres Opérationnels Départementaux (COD). En situation de crise, la continuité des communications et l'accès aux outils métier sont essentiels pour assurer une gestion efficace des interventions. Or, plusieurs retours d'expérience ont révélé des défaillances critiques, notamment des coupures d'Internet ou de téléphonie, rendant la coordination difficile.

L'objectif principal du projet INFRASEC est de mettre en œuvre une solution technique complète, résiliente et sécurisée, permettant à la fois un fonctionnement optimal du COD en interne, et un accès distant fiable pour les agents de terrain. Cette solution inclut la redondance des accès réseau, la mise en place d'un VPN, un système de téléphonie IP, une messagerie locale, une supervision des serveurs et l'intégration du logiciel open source **eBrigade**.

En combinant haute disponibilité, supervision proactive et sécurité des accès, le projet INFRASEC répond aux exigences croissantes des dispositifs de sécurité civile et contribue à renforcer la capacité de réponse opérationnelle du service interministériel en charge des systèmes d'information. Il sera d'abord mis en œuvre en environnement virtuel à des fins de test, avant un éventuel déploiement réel.

Besoins et contraintes

Les besoins exprimés portent sur l'amélioration de l'infrastructure IT afin de garantir la continuité et la sécurité des services. Il est essentiel d'assurer la haute disponibilité des services critiques en mettant en place des solutions de redondance et de bascule automatique. La mise en œuvre d'une solution de redondance des accès Internet permettra d'éviter les interruptions en cas de panne d'un fournisseur. De plus, un VPN sécurisé devra être déployé afin de garantir des connexions sûres pour les agents sur le terrain. L'installation d'une solution de téléphonie VoIP optimisera les communications internes et externes, tandis que la supervision des serveurs et équipements critiques assurera une surveillance proactive des infrastructures. Enfin, le déploiement d'une messagerie professionnelle fiable et sécurisée facilitera la communication et la collaboration au sein de l'organisation.

Objectifs techniques

1. Redondance et Sécurité :
   - Mise en place d'un pare-feu **PfSense** avec haute disponibilité
   - Redondance des routeurs et liens WAN (double accès Internet)
2. Connexion à distance sécurisée :
   - **OpenVPN Road Warrior** pour permettre aux agents un accès sécurisé aux outils métiers
3. Supervision et Monitoring :
   - Supervision des serveurs et équipements critiques avec alertes en cas de panne
4. Infrastructure réseau et gestion des utilisateurs :
   - **Windows Server 2022** pour la gestion de l'Active Directory et des ressources
5. Téléphonie IP :

- Serveur VoIP avec des clients softphones pour la communication

6. Hébergement des services :
   - Ubuntu Serveur pour l'hébergement des services Open Source
7. Messagerie professionnelle

Solutions retenues et argumentations

1. Active directory, services DNS et DHCP

Solution retenue :

Déploiement de deux serveurs Active Directory (AD) (un principal, un secondaire) hébergeant également les services DNS et DHCP.

L'Active Directory offre une gestion centralisée et sécurisée des utilisateurs, groupes et stratégies de sécurité, tout en permettant une authentification unique (SSO) sur l'ensemble des services. En hébergeant les services DNS et DHCP sur les mêmes serveurs, on assure une cohérence dans la gestion du réseau, une résolution des noms fiable et une attribution automatique des adresses IP. La redondance (principal/secondaire) garantit la disponibilité même en cas de panne d'un serveur, point essentiel en contexte de crise.

2. Téléphonie IP (VoIP)

Solution retenue :

Serveur Asterisk (open source) avec clients softphone (Zoiper) sur les postes utilisateurs.

Asterisk est une solution éprouvée et largement utilisée dans les environnements critiques. Elle offre flexibilité, compatibilité avec de nombreux équipements et une gestion avancée des communications (transferts, messagerie vocale, groupes d'appels). Les softphones permettent une utilisation sur site et à distance via VPN, sans surcoût matériel supplémentaire. Cela garantit la continuité des échanges, y compris en cas de coupure des lignes classiques.

3. Messagerie électronique interne

Solution retenue :

Déploiement du serveur de messagerie open source Modoboa, accessible uniquement via le réseau interne (LAN) ou par VPN.

Modoboa est une plateforme moderne, complète et open source qui intègre la gestion des comptes, des domaines, du webmail et des outils d'administration. Elle s'appuie sur des solutions et offre une protection avancée contre les spams et virus. En l'intégrant à l'Active Directory, on centralise la gestion des identités. Le choix d'une solution interne garantit la confidentialité, l'autonomie vis-à-vis des services extérieurs et la résilience en cas de rupture de la connectivité Internet.

4. Supervision et monitoring

Solution retenue :

Outil de supervision PRTG Network Monitor.

PRTG est reconnu pour sa simplicité de déploiement, son interface graphique intuitive et ses capacités de supervision en temps réel. Il permet de surveiller la disponibilité et les performances de tous les équipements critiques (serveurs, routeurs, liens WAN, etc.), d'envoyer des alertes automatiques par e-mail ou SMS en cas d'incident, et de générer des rapports historiques détaillés. Cela permet aux

administrateurs d'être immédiatement avertis d'une anomalie et d'anticiper les pannes, ce qui est crucial pour une infrastructure de sécurité civile.

5. Logiciel de gestion des interventions

Solution retenue :

Déploiement du logiciel open source eBrigade sur un serveur web sécurisé, accessible en LAN et via DMZ. eBrigade permet la gestion complète des interventions, du personnel, des ressources matérielles et des mains courantes. L'accès en temps réel aux informations opérationnelles, depuis la salle de crise ou le terrain (via VPN/DMZ), facilite la coordination et la réactivité des équipes. Son adoption permet également de dématérialiser les rapports et de centraliser la documentation liée aux événements.

6. Connexion sécurisée à distance

Solution retenue :

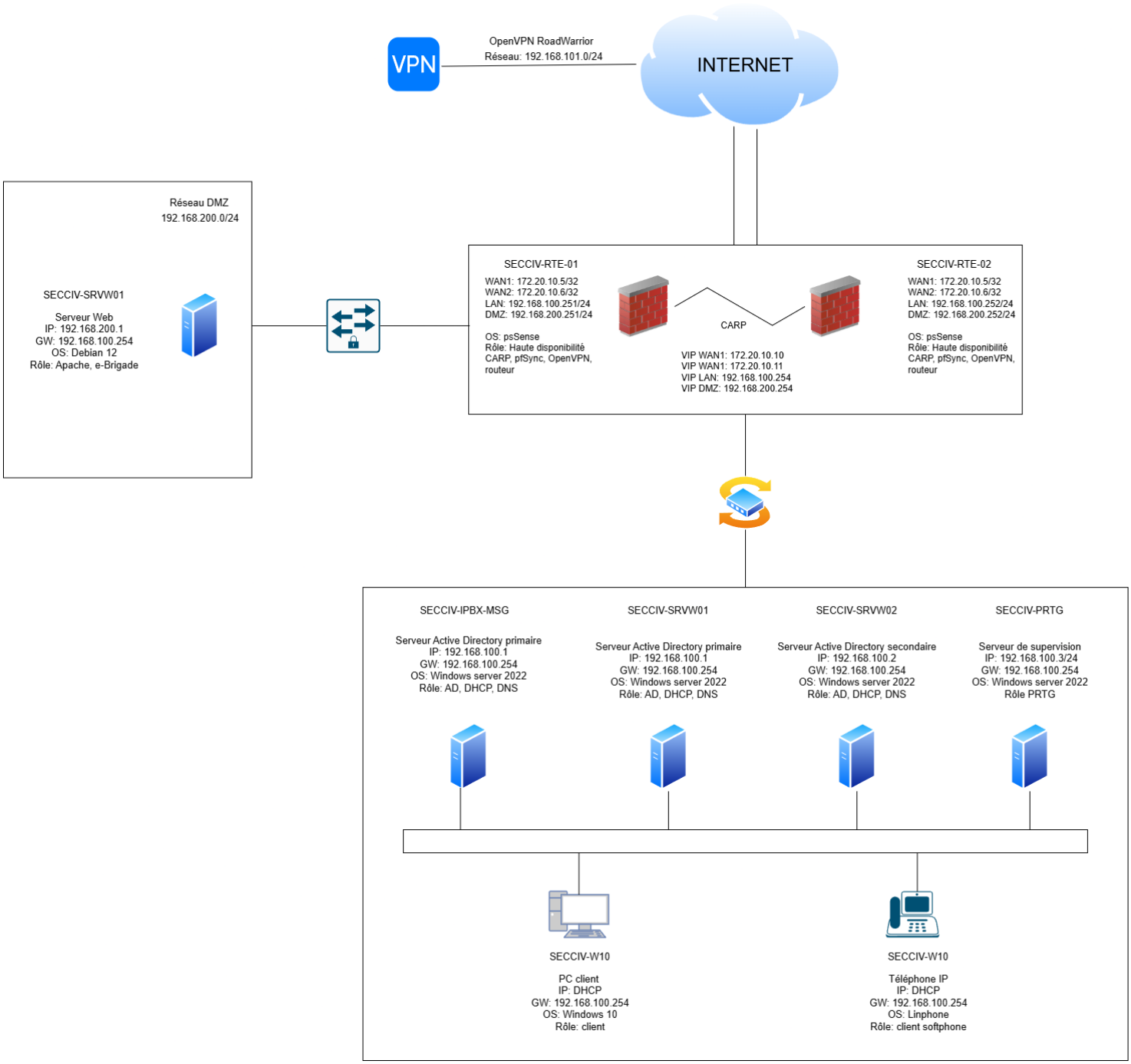
Mise en place d'un VPN OpenVPN Road Warrior, avec authentification via l'Active Directory. OpenVPN garantit la confidentialité et l'intégrité des échanges entre les agents sur le terrain et le COD. L'authentification centralisée via AD renforce la sécurité, en permettant de contrôler précisément qui accède aux ressources sensibles. Le VPN permet aussi d'utiliser l'ensemble des services internes (messagerie, VoIP, eBrigade) comme si l'agent était sur site, assurant ainsi une continuité opérationnelle.

7. DMZ sécurisée

Solution retenue :

Création d'une DMZ isolée, protégée par un pare-feu (pfSense), pour héberger le serveur web eBrigade. La DMZ permet d'ouvrir un accès contrôlé à eBrigade depuis l'extérieur tout en protégeant le réseau interne d'éventuelles attaques. Des règles de pare-feu strictes limiteront les flux aux ports/services indispensables, réduisant la surface d'exposition. Cela répond à la nécessité d'un accès en mode dégradé en cas de coupure VPN, tout en respectant les exigences de sécurité.

Schéma réseau



Coût du projet

Ressources humaines

Description	Utilisé	Commentaires
Nombre de personnes mobilisées	2 (binôme)	Stable sur toute la durée
Temps de travail total	~90 heures	Gain de temps sur certaines tâches grâce à une bonne préparation
Jours de travail estimés	12 jours/homme	Temps effectif mieux maîtrisé

Certaines phases comme l'étude du cahier des charges et la configuration des outils open source se sont révélées particulièrement efficaces, notamment grâce à une bonne répartition des tâches. En revanche, la rédaction de la documentation a demandé plus d'efforts que les autres volets techniques.

Ressources financières

Description	Utilisé (simulé)	Commentaires
Matériel (serveurs, routeurs)	26 700 €	Conformité totale au devis
Licences / Logiciels	300 €	Aucun surcoût (logiciels open source utilisés)
Main-d'œuvre	~9 000 €	Moins d'heures consommées que prévu
Total HT	~36 000 €	Légère économie réalisée

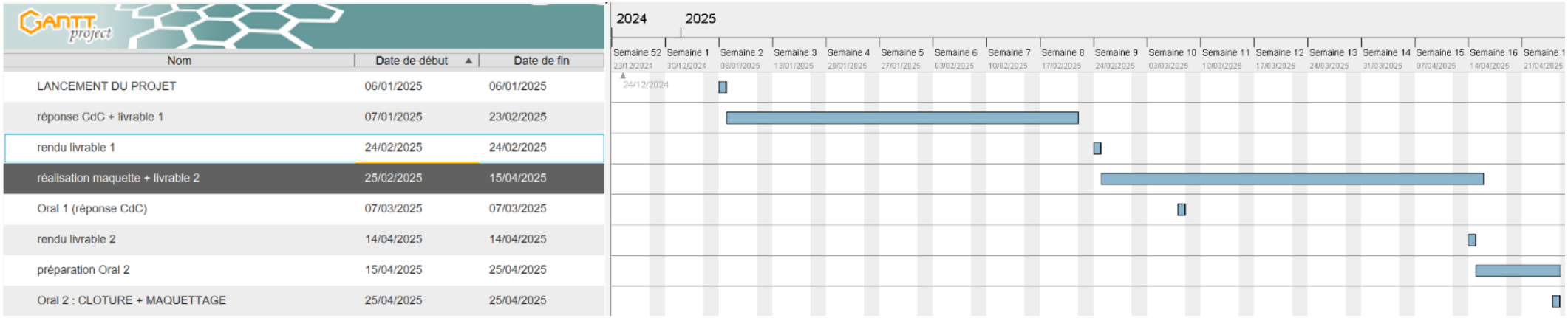
La maîtrise des coûts s'explique par le recours à des solutions open source (Asterisk, Modoboa, eBrigade, pfSense…) et une optimisation du temps de configuration. Aucune dépense non planifiée n'a été nécessaire.

Ressources organisationnelles et techniques

Ressource	Utilisée	Observations
Environnement de test virtuel	Oui	Suffisant pour toutes les phases
Support pédagogique (formateurs)	Oui	Sollicités à plusieurs étapes clés
Accès aux ressources réseau (VPN, DMZ…)	Oui	Toutes les fonctionnalités ont été déployées avec succès

Le projet a bénéficié d'un bon encadrement et d'une infrastructure virtuelle adaptée. La coordination et la gestion des ressources techniques ont permis un déroulement fluide tout au long du projet.

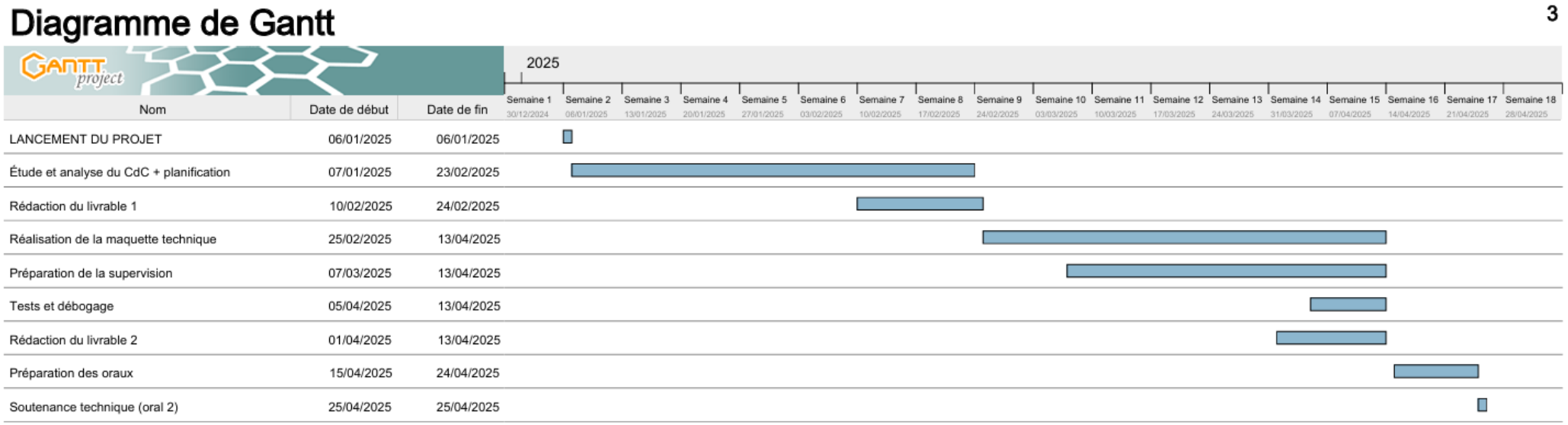
Planning prévisionnel



Nom	Date de début	Date de fin
LANCEMENT DU PROJET	06/01/2025	06/01/2025
réponse CdC + livrable 1	07/01/2025	23/02/2025
rendu livrable 1	24/02/2025	24/02/2025
réalisation maquette + livrable 2	25/02/2025	15/04/2025
Oral 1 (réponse CdC)	07/03/2025	07/03/2025
rendu livrable 2	14/04/2025	14/04/2025
préparation Oral 2	15/04/2025	25/04/2025
Oral 2 : CLOTURE + MAQUETTAGE	25/04/2025	25/04/2025

Le planning prévisionnel du projet INFRASEC s'étale du 6 janvier au 25 avril 2025, structuré en plusieurs phases clés. Après le lancement officiel, l'équipe a travaillé sur l'analyse du cahier des charges et la préparation du livrable 1, remis le 24 février. La phase de réalisation de la maquette technique s'est ensuite déroulée du 25 février au 15 avril, incluant le déploiement des services, les tests et la production de la documentation. Un oral intermédiaire a eu lieu le 7 mars pour valider l'avancement. Enfin, la dernière partie du projet a été consacrée à la finalisation du livrable 2, à la préparation de la soutenance, puis à la présentation technique clôturant officiellement le projet le 25 avril. Ce planning a permis une gestion fluide et séquencée du projet, avec un bon équilibre entre phases de conception, d'implémentation et de validation.
4o

Planning réel



Nom	Date de début	Date de fin
LANCEMENT DU PROJET	06/01/2025	06/01/2025
Étude et analyse du CdC + planification	07/01/2025	23/02/2025
Rédaction du livrable 1	10/02/2025	24/02/2025
Réalisation de la maquette technique	25/02/2025	13/04/2025
Préparation de la supervision	07/03/2025	13/04/2025
Tests et débogage	05/04/2025	13/04/2025
Rédaction du livrable 2	01/04/2025	13/04/2025
Préparation des oraux	15/04/2025	24/04/2025
Soutenance technique (oral 2)	25/04/2025	25/04/2025

Le projet **INFRASEC**, dans sa réalisation concrète, a suivi une progression très proche du planning initial, avec de légers ajustements. Le projet a débuté le **6 janvier 2025** avec la réunion de lancement, suivie d'une **phase d'étude du cahier des charges et de planification** du 7 janvier au 23 février. La **rédaction du livrable 1** s'est étendue du 10 au 24 février, en parallèle de la phase d'analyse.

La **maquette technique** a été développée du 25 février au 13 avril, accompagnée par la **mise en place de la supervision** (7 mars au 13 avril), les **tests et débogages** (5 au 13 avril), et la **rédaction du livrable 2** (1er au 13 avril). La **préparation des oraux** s'est déroulée du 15 au 24 avril, avec la **soutenance technique finale** le 25 avril 2025. Toutes les phases ont été menées dans les temps, sans glissement majeur.

Planning prévisionnel vs réel

Le planning initial du projet Sécurité Civile prévoyait une réalisation s'étalant du 6 janvier au 25 avril 2025, avec deux livrables majeurs et une démonstration technique à finaliser en phase terminale. L'ensemble des jalons fixés ont été respectés dans les grandes lignes, mais certains ajustements ont été nécessaires sur des tâches spécifiques.

Tâche	Date prévue	Date réelle	Écart constaté	Analyse
Lancement du projet	06/01/2025	06/01/2025	Aucun	Conforme au planning
Étude du CdC & choix techniques	07/01 – 23/02/2025	07/01 – 20/02/2025	3 jours d'avance	Le CdC était clair, aucune difficulté rencontrée
Rédaction livrable 1	jusqu'au 24/02/2025	jusqu'au 24/02/2025	Aucun	Tâche réalisée dans les temps
Réalisation de la maquette	25/02 – 13/04/2025	25/02 – 10/04/2025	3 jours d'avance	Bonne anticipation des configurations, peu d'imprévus
Rédaction livrable 2	01/04 – 13/04/2025	05/04 – 13/04/2025	Légère dérive (démarrage tardif)	Début ralenti par des ajustements techniques
Préparation oraux	15/04 – 24/04/2025	En cours	Conforme (prévision)	Aucun dérapage constaté à date
Soutenance (oral 2)	25/04/2025	25/04/2025	À venir	Planning maintenu

Analyse des dérives ou écarts

Cas d'avance :

- Certaines tâches ont été finalisées plus tôt que prévu, notamment l'étude du cahier des charges et la configuration initiale de la maquette.
- Cela s'explique par une bonne préparation en amont, des choix techniques simples à mettre en œuvre (solutions open source bien documentées), et une répartition efficace du travail.

Cas de dérive :

- La rédaction du livrable 2 a connu un démarrage légèrement retardé, dû à :
  - Des ajustements de dernière minute sur la supervision (PRTG),
  - Une mauvaise estimation du temps nécessaire à la documentation technique.
- Cause anticipable : la rédaction a été sous-estimée au profit de la configuration technique.
- Mesures préventives pour l'avenir :
  - Prévoir une marge pour les tâches de documentation.
  - Démarrer la documentation en parallèle de la réalisation technique.

Résultats attendus VS Résultats obtenus

Objectif initial	Résultat obtenu	Écart / Commentaire
Haute disponibilité du réseau (redondance routeurs et accès WAN)	Simulée avec deux routeurs virtuels et un accès WAN	Objectif atteint
Mise en place de deux serveurs Active Directory (AD principal + secondaire)	Réalisé avec synchronisation fonctionnelle	Aucun écart constaté
Hébergement des services DNS et DHCP via AD	Fonctionnels et bien intégrés à l'infrastructure	Bonne cohérence réseau
Déploiement d'un serveur de téléphonie IP (Asterisk) avec clients softphone	Fonctionnel en local et via VPN	Objectif atteint sans complexité majeure
Installation d'une messagerie interne	Changement de solution : Exchange → Modoboa	Problème contourné efficacement, adaptation réussie
Mise en place d'une supervision système	Réalisée avec PRTG	Système stable et lisible
Déploiement de l'application eBrigade accessible en LAN et via DMZ	Installation et accès conforme	Réussite complète, solution recommandée
Configuration d'un VPN Road Warrior sécurisé	Fonctionnel après ajustements réseau	Problème initial de routage résolu
Accès sécurisé aux ressources via VPN (eBrigade, mail, téléphonie)	Accès complet une fois la connexion établie	Objectif atteint
Documentation complète et livrables à jour	Réalisés et remis dans les délais	Quelques ajustements mineurs sur la forme

La majorité des objectifs techniques fixés dans le projet INFRASEC ont été atteints avec succès. L'infrastructure réseau prévue a bien été simulée avec une haute disponibilité, les services Active Directory, DNS et DHCP ont été correctement déployés et intégrés. La messagerie a dû être adaptée en cours de projet, avec un passage d'Exchange à Modoboa, choix judicieux au vu des contraintes techniques. Tous les services critiques (VPN, téléphonie, eBrigade, supervision) sont fonctionnels, accessibles et bien intégrés entre eux. Enfin, la documentation et les livrables ont été remis dans les délais, malgré quelques ajustements de forme. Le projet a donc répondu aux attentes, avec une bonne capacité d'adaptation face aux imprévus.

Conclusion

Le projet INFRASEC avait pour ambition de concevoir et de mettre en œuvre une infrastructure informatique résiliente, capable d'assurer la continuité des services critiques du Centre Opérationnel Départemental (COD) en situation de crise.

Grâce à une analyse approfondie du cahier des charges, des choix techniques adaptés et une organisation efficace, l'ensemble des objectifs fixés ont été atteints. Les technologies déployées (Active Directory, VPN, messagerie, téléphonie IP, supervision, eBrigade) ont permis de créer un système cohérent, sécurisé, et facilement administrable. Malgré quelques ajustements en cours de projet, notamment sur le choix de la messagerie ou la configuration du VPN, les problèmes ont été rapidement identifiés et corrigés.

Ce projet a été une réelle opportunité de mettre en pratique des compétences variées en systèmes et réseaux, tout en développant une rigueur de gestion de projet. Il a permis de mieux comprendre les enjeux de la résilience informatique en environnement sensible, ainsi que l'importance de la communication, de la planification et de la documentation dans la réussite d'un projet technique.
En conclusion, le projet INFRASEC a été une réussite, tant sur le plan technique que pédagogique, et constitue une base solide pour des projets similaires dans un cadre professionnel réel.

Améliorations possibles

Plusieurs pistes d'amélioration ont été identifiées à l'issue du projet INFRASEC, afin d'optimiser davantage la solution mise en place. Sur le plan du monitoring, il serait pertinent d'ajouter des sondes de tests utilisateurs ou des sondes spécifiques aux services critiques (eBrigade, messagerie, téléphonie) pour affiner la surveillance et détecter plus rapidement les incidents. En matière de sécurité, la mise en œuvre d'une authentification à deux facteurs pour l'accès VPN renforcerait considérablement la protection des accès distants, notamment dans un contexte sensible de sécurité civile. Enfin, pour améliorer l'expérience utilisateur.